

国際調査報告

(法8条、法施行規則第40、41条)
〔PCT18条、PCT規則43、44〕

Done

出願人又は代理人 の書類記号 P23892	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。		
国際出願番号 PCT/JPO0/06355	国際出願日 (日.月.年) 18.09.00	優先日 (日.月.年) 16.09.99	
出願人 (氏名又は名称) 松 下 電 器 産 業 株 式 会 社			

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 5 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☐ 出願人が提出したものを承認する。

☒ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 13 図とする。 ☐ 出願人が示したとおりである。

☐ なし

☒ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

THIS PAGE BLANK (USPTO)

第Ⅲ欄 要約 (第1ページの5の続き)

複数回使用可能なチケットに対応したローカルなデジタル署名メカニズムをもつ効率的な電子財布を提供する。チケットは、電子バリューオブジェクトであり、バリューを表すバリュー属性記述部(800)、改札処理を指定するサービス制御部(803)、このオブジェクトに対する固有の秘密鍵を格納するセキュリティ情報部(804)、などから構成される。これらの部分はそれぞれサービス提供者によって署名されている。ただし、バリュー属性記述部の可変属性(802)たとえば残り回数は前記の秘密鍵により署名されており、この残り回数は改札時にデクリメントされ秘密鍵によって署名しなおされる。

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁷ G06F 17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁷ G06F 17/60 G06F 19/00 G07F 7/08 G09C 1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926 - 1996 年
 日本国公開実用新案公報 1971 - 2000 年
 日本国実用新案登録公報 1996 - 2000 年
 日本国登録実用新案公報 1994 - 2000 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WAYNER, Peter, <i>Digital Cash: Commerce on the Net</i> , 2nd edition, April 1 1997 (01.04.97), Academic Press (London, UK). pp. 212-213 の "Migration" セクションを見よ (特に "For instance, the first batch of ..." と "Mondex clearly anticipates updating..." の段落).	1
X	WO, 99/09502, A1 (松下電器産業株式会社) 25.2 月.1999 (25.02.99) & AU, 86484/98, A1 & CN, 1246941, A	18-20, 25, 26

☒ C 欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

12.12.00

国際調査報告の発送日

26.12.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
 郵便番号 100-8915
 東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官 (権限のある職員)

阿波 進



5 L

9168

電話番号 03-3581-1101 内線 3561

THIS PAGE BLANK (USPTO)

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	& EP, 950968, A1 & JP, 99/09502, A1 図 109(b)と 110(a)(b)を見よ(特に[10915]と[11006]; cf. 図 19 [1098]).	
X	JP, 11-225143, A (富士ゼロックス株式会社) 17.8 月.1999 (17.08.99) (ファミリーなし) 実施例 2 および 3 の記述を見よ(特に M, M', および x の扱いについて).	25
A	JP, 11-031204, A (富士ゼロックス株式会社) 2.2 月.1999 (02.02.99) (ファミリーなし) 「第 3 のプロトコル」の記述を見よ(特に i と in の扱いについて).	1-35
A	GLASSMAN, Steve <i>et al</i> , "The Millicent Protocol for Inexpensive Electronic Commerce", in <i>World Wide Web Journal—Fourth International World Wide Web Conference</i> , December 1995, O'Reilly & Associates (Sebastopol, USA). Appendix を見よ(特に "Authentic and private" の項目).	1-35
A	EP, 917120, A2, A3 (Citicorp Development Center Inc) 19. 5 月. 1999 (19.05.99) & AU, 92346/98, A1 & AU, 17965/99, A1 & AU, 15844/99, A1 & BR, 98/06416, A & CN, 1233804, A & EP, 951158, A2 & EP, 950992, A2, A3 & EP, 917119, A2 & JP, 11-232348, A & JP, 11-250165, A & WO, 99/24891, A2 & WO, 99/24891, A2 図 3 を見よ(特に 2 つの "applications container" について).	1-35
A	FINGAR, Peter <i>et al</i> , "The Business of Distributed Object Computing",	1-35

THIS PAGE BLANK (USPTO)

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 -	関連する 請求の範囲の番号
	in <i>Object Magazine</i> , April 1997 (04.97). “ <i>The bottom layers provides ...</i> ” の段落を見よ.	

THIS PAGE BLANK (USPTO)



特許協力条約に基づいて公開された国際出願



(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年3月22日 (22.03.2001)

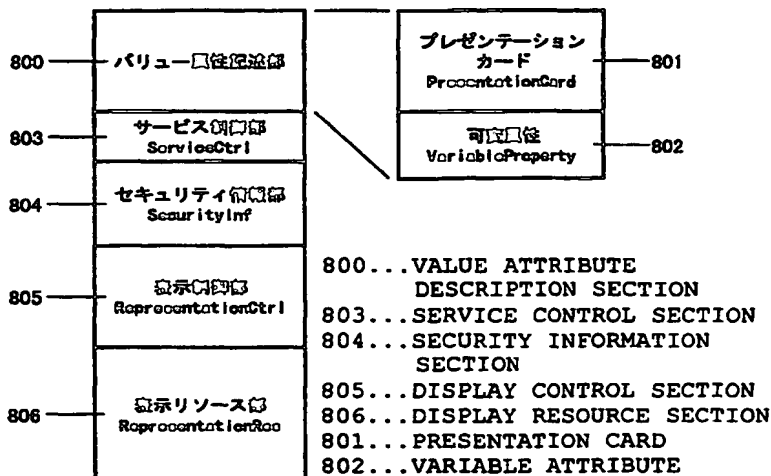
PCT

(10) 国際公開番号
WO 01/20509 A1

- (51) 国際特許分類: G06F 17/60 世田谷区松原 5-6-12 Tokyo (JP). 松瀬哲朗 (MATSUSE, Tetsuo) [JP/JP]; 〒565-0853 大阪府吹田市春日 2-6-3-109 Osaka (JP). 川口京子 (KAWAGUCHI, Kyoko) [JP/JP]; 〒271-0093 千葉県松戸市小山 705-1-207 Chiba (JP). 中西良明 (NAKANISHI, Yoshiaki) [JP/JP]; 〒166-0014 東京都杉並区松ノ木 2-4-10-305 Tokyo (JP). 佐々木理 (SASAKI, Osamu) [JP/JP]; 〒144-0046 東京都大田区東六郷 2-20-5-620 Tokyo (JP).
- (21) 国際出願番号: PCT/JP00/06355
- (22) 国際出願日: 2000年9月18日 (18.09.2000)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願平11/262766 1999年9月16日 (16.09.1999) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真 1006 番地 Osaka (JP).
- (74) 代理人: 弁理士 蔵合正樹, 外 (ZOGO, Masahiro, et al.); 〒102-0083 東京都千代田区麹町 5 丁目 7 番地 秀和 紀尾井町 TBR ビル Tokyo (JP).
- (81) 指定国 (国内): CN, JP, US.
- (84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB, IT).
- 添付公開書類:
— 国際調査報告書
- (72) 発明者: および
- (75) 発明者/出願人 (米国についてのみ): 高山 久 (TAKAYAMA, Hisashi) [JP/JP]; 〒156-0043 東京都
- 2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: ELECTRONIC WALLET

(54) 発明の名称: 電子財布



(57) Abstract: An efficient electronic wallet having local digital signature mechanism adapted to a ticket usable a plurality of times. The ticket is an electronic value object comprising a value attribute description section (800) representing the value, a service control section (803) for specifying a ticket examination, and a security information section (804) where a secret key specific to the object is stored. The service provider signs these sections. A variable attribute (802) of the value attribute description section (800) such as the number of remaining times is signed with the secret key. The number is decremented when the ticket is examined and re-signed with the secret key.

[続表有]



(57) 要約:

複数回使用可能なチケットに対応したローカルなデジタル署名メカニズムをもつ効率的な電子財布を提供する。チケットは、電子バリューオブジェクトであり、バリューを表すバリュー属性記述部(800)、改札処理を指定するサービス制御部(803)、このオブジェクトに対する固有の秘密鍵を格納するセキュリティ情報部(804)、などから構成される。これらの部分はそれぞれサービス提供者によって署名されている。ただし、バリュー属性記述部の可変属性(802)たとえば残り回数は前記の秘密鍵により署名されており、この残り回数は改札時にデクリメントされ秘密鍵によって署名しなおされる。

明 細 書

電子財布

技術分野

本発明は、プリペイドカードやクレジットカード（バンクカード）に代表される小売販売取引における決済機能、各種イベント、公演、映画等のチケットの改札機能、さらには、それら、プリペイドカードやチケットの流通・販売機能を提供するエレクトロニックコマースシステムに関し、特に、利便性と、決済の安全性を担保し、効率的で、円滑な商取引を可能にするものである。

背景技術

近年、電子マネーや電子チケットなど価値情報を電子化し、流通を効率化しようとする取り組みが行われている。

その一つの方式として、その価値情報が持つ属性をマークアップ記述言語で規定して、それに所有者のデジタル署名を施すことによって、流通を可能にする方式がある。図1（a）は、従来技術における価値情報の発行者のセンターサーバ3300からユーザのICカード3301に、電子化された価値情報3303が発行された状態を示す模式図である。ICカード3300に格納された価値情報3303は、マークアップ記述言語によって、価値情報が持つ属性が記述されており、不正な改竄を防止するため、全体に対して発行者(Issuer)によるデジタル署名が施されている。また、図1（b）は、従来技術における電子化された価値情報3303がマーチャントに対して使用された状態を示す模式図である。マーチャント端末3302に格納されている価値情報3304は、ICカード3300に格納されていた価値情報3303に、所有者の変更を示す情報を付加し、不正な改竄を防止するため、ユーザ(User)によるデジタル署名が施されたものである。情報は変更せず、追加するだけなので、改竄等の不正行為に対す安全性が高く、電子化された価値情報を安全に流通させることが出来る方式である。

また、このような電子化された価値情報が格納されたICカードを携帯端末に装着し、携帯端末と小売店側のPOS端末との間で、代金に支払い等の決済処理を、ブルーツースと呼ばれるのローカル無線通信によって行う決済方式が提案されている。

しかしながら、従来の方式では、電子化された価値情報が流通する度に、電子化された価値情報のデータサイズが大きくなってしまい、取り扱いが不便であった。

また、従来の方式では、電子化された価値情報を流通させる時に、双方の証明書を交換してデジタル署名を検証する必要があり、匿名性が確保できないという課題があった。

また、従来の方式では、価値情報の種類により電子化の方式が異なり、例えば、プリペイドカードやチケットを統一的に取り扱うことができないという課題があった。

また、従来の方式では、電子化された価値情報をＩＣカードに格納するため、電子化された価値情報のデータ容量が限定され、画像情報などのマルチメディア情報を含めることができず、価値情報の表現力という点において課題があった。さらに、従来の方式では、決済処理を開始する前に、ブルーツース（ブルーツース）によって通信する相手を特定する必要があり、特に、複数台のＰＯＳ端末が並んで設置されているような場合、相手のＰＯＳ端末の識別番号を入力するなどの煩雑な操作をする必要があった。

発明の開示

本発明は、こうした従来の技術の課題を解決するもので、その第１の目的は、匿名性と安全性、および利便性に優れ、価値情報を効率的に電子化して電子バリューを生成することができる電子財布を提供することである。

本発明の第２の目的は、各種の電子化された価値情報をユーザが効率的に取り扱うことが出来る電子財布を提供することである。

本発明は上記目的を達成するために、電子情報を、秘密鍵と証明書と、その秘密鍵を使ってサービスの提供者（すなわち本発明の電子財布システムの提供者）により署名された情報とを備えたデータ構成となし、この電子情報を保存管理する手段を電子財布に備えたものである。すなわち、本発明では、電子財布（電子的価値情報の取得、格納、管理、およびデータの変更を行う）に格納される電子情報のそれぞれに、各々固有の秘密鍵が組み込まれており、この秘密鍵を解除して初めて電子情報内部の価値情報が開かれるようにしている。

このため、電子情報の有効性がそれ自身で証明される。また、仮に1つの電子情報の秘密鍵が第三者によって破られたとしても、それ以外の電子情報はまた別の秘密かび、証明書、および秘密鍵による署名によってガードされているから匿名性が高いレベルで確保される。

図面の簡単な説明

第1図

(a) 従来の技術における電子化された価値情報が発行された状態を示す模式図である。

(b) 従来の技術における電子化された価値情報が使用された状態を示す模式図である。

第2図

本発明による電子財布の基本構造を表す図である。

第3図

第2図に示す電子財布において、秘密鍵で署名された情報が可変情報であることを示す図である。

第4図

第3図に示す電子財布に格納される電子情報が、さらに電子情報の発行者によって署名された情報を有している構成を示す図である。

第5図

第4図に示す電子財布において、秘密鍵で署名された情報が可変情報であり、また、電子情報の発行者によって署名された情報が固定情報であることを示す図である。

第6図

本発明の第1の実施例におけるモバイル・エレクトロニックコマース・システムのブロック構成図である。

第7図

(a) 本発明の第1の実施例におけるモバイルユーザ端末の前面の概観図である。

(b) 本発明の第1の実施例におけるモバイルユーザ端末の背面の概観図であ

る。

第 8 図

本発明の第 1 の実施例におけるモバイルユーザ端末のブロック構成図である。

第 9 図

本発明の実施例におけるモバイルユーザ端末のアプリケーションと他の構成要素と、他の機器との関係を示す模式図である。

第 10 図

(a) 本発明の実施例におけるモバイルユーザ端末の電源オン時の画面の概観図である。

(b) 本発明の実施例におけるモバイルユーザ端末のインターネットメニュー画面の概観図である。

(c) 本発明の実施例におけるモバイルユーザ端末の電子バリューのオーダー画面の概観図である。

(d) 本発明の実施例におけるモバイルユーザ端末のパスワード入力画面の概観図である。

(e) 本発明の実施例におけるモバイルユーザ端末の電子バリューの一覧画面の概観図である。

(f) 本発明の実施例におけるモバイルユーザ端末の電子バリュー表示画面の概観図である。

(g) 本発明の実施例におけるモバイルユーザ端末の電子バリュー受信操作画面の概観図である。

第 11 図

本発明の第 1 の実施例におけるサービス端末のブロック構成図である。

第 12 図

本発明の第 1 の実施例におけるユーザ端末のブロック構成図である。

第 13 図

本発明の第 1 の実施例における電子バリューのデータ構造の模式図である。

第 14 図

本発明の第 1 の実施例における電子バリューハンドラーのデータ構造の模式図

である。

第 15 図

本発明の第 1 の実施例における改札決済処理において交換されるメッセージの模式図である。

第 16 図

(a) 本発明の第 1 の実施例における改札決済処理のメッセージプレゼンテーションのデータ構造の模式図である。

(b) 本発明の第 1 の実施例における改札決済処理のメッセージインストラクションのデータ構造の模式図である。

(c) 本発明の第 1 の実施例における改札決済処理のメッセージトランザクションのデータ構造の模式図である。

(d) 本発明の第 1 の実施例における改札決済処理のメッセージ Receipt のデータ構造の模式図である。

(e) 本発明の第 1 の実施例における改札決済処理のメッセージアクノードのデータ構造の模式図である。

第 17 図

本発明の第 1 の実施例における電子財布に登録されている電子バリューのマークアップ記述言語による記述の模式図である。

第 18 図

本発明の第 1 の実施例における電子バリューのプレゼンテーションカードと可変属性のマークアップ記述言語による記述の模式図である。

第 19 図

本発明の第 1 の実施例における電子バリューのサービス制御部とセキュリティ情報部のマークアップ記述言語による記述の模式図である。

第 20 図

本発明の第 1 の実施例における電子バリューの表示制御部のマークアップ記述言語による記述の模式図である。

第 21 図

本発明の第 1 の実施例における電子バリューの表示リソース部のマークアップ

記述言語による記述の模式図である。

第 2 2 図

本発明の第 1 の実施例における電子バリューオブジェクトが生成する”Main”の画面情報の模式図である。

第 2 3 図

本発明の第 1 の実施例における電子バリューハンドラのマークアップ記述言語による記述の模式図である。

第 2 4 図

(a) 本発明の第 1 の実施例における改札決済処理のメッセージプゼンテーション中のサービス制御メッセージのデータ構造の模式図である。

(b) 本発明の第 1 の実施例における改札決済処理のメッセージインストラクション中のサービス制御メッセージのデータ構造の模式図である。

(c) 本発明の第 1 の実施例における改札決済処理のメッセージトランザクション中のサービス制御メッセージのデータ構造の模式図である。

(d) 本発明の第 1 の実施例における改札決済処理のメッセージ Receipt 中のサービス制御メッセージのデータ構造の模式図である。

第 2 5 図

本発明の第 1 の実施例における改札決済処理後の電子バリューの可変属性のマークアップ記述言語による記述の模式図である。

第 2 6 図

本発明の第 1 の実施例における情報提供サーバからブラウザに送信される電子バリューの受信操作を促すデータの模式図である。

第 2 7 図

本発明の第 1 の実施例における電子バリュー発行サーバのブロック構成図である。

第 2 8 図

本発明の第 1 の実施例における電子バリューテンプレートデータベースに管理されている一つの電子バリューテンプレートデータ 2300 の構成の模式図である。

第 2 9 図

(a) 本発明の第 1 の実施例における電子バリューの発行の手順を示すフロー図である。

(b) 本発明の第 1 の実施例における電子バリューの表示制御部と表示リソース部のダウンロードの手順を示すフロー図である。

第 3 0 図

(a) 本発明の第 1 の実施例における電子バリュー発行要求のマークアップ記述言語による記述の模式図である。

(b) 本発明の第 1 の実施例における端末プロファイルのマークアップ記述言語による記述の模式図である。

第 3 1 図

本発明の第 1 の実施例における電子バリュー発行サーバによる電子バリューの生成処理のフロー図である。

第 3 2 図

本発明の第 1 の実施例における電子バリュー発行サーバの電子バリューデータベースに登録されている電子バリューのマークアップ記述言語による記述の模式図である。

第 3 3 図

(a) 本発明の第 2 の実施例におけるモバイルユーザ端末の前面の概観図である。

(b) 本発明の第 2 の実施例におけるモバイルユーザ端末の背面の概観図である。

第 3 4 図

本発明の第 2 の実施例におけるモバイルユーザ端末のブロック構成図である。

第 3 5 図

本発明の第 2 の実施例におけるサービス端末のブロック構成図である。

第 3 6 図

(a) 本発明の第 2 の実施例におけるパターン 1 の場合のモバイルユーザ端末の改札決済処理のフロー図である。

(b) 本発明の第 2 の実施例におけるパターン 1 の場合のサービス端末の改札決

済処理のフロー図である。

第 3 7 図

(a) 本発明の第 2 の実施例におけるパターン 2 の場合のモバイルユーザ端末の改札決済処理のフロー図である。

(b) 本発明の第 2 の実施例におけるパターン 2 の場合のサービス端末の改札決済処理のフロー図である。

発明の好ましい実施の態様

図 2 は、本発明による電子財布の基本構造を表す図である。この図に示されているように、電子財布 1 は価値情報を含んだ電子情報を保存し管理する電子情報保存管理手段 2 を備えており、このにおいて電子情報保存管理手段 2 には電子情報 3 が格納されている。電子情報 3 は、この電子情報のデータ本体をなす価値情報に加えて、その電子情報 3 に固有の秘密鍵 4 とその証明書 5 の組と、その秘密鍵によって署名された情報 6 とを備えて成る。この図 1 では電子情報保存管理手段 2 の中には 1 つの電子情報 3 しか表されていないが、通常は、電子情報保存管理手段 2 の中には複数の電子情報 3 が格納される。このように、電子情報 3 の中に秘密鍵 4 と証明書 5 とを組み込んでいることにより、電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

図 3 は、図 2 に示す電子財布 1 において、秘密鍵 4 で署名された情報が可変情報であることを示す図である。電子情報 3 は、その電子情報 3 に固有の秘密鍵 4 とその証明書 5 の組と、その秘密鍵 4 によって署名された可変情報 7 とを備えて成る。このように秘密鍵 4 によって可変情報 7 が署名されるため、情報を可変する、すなわちデータの書き換えが行なわれる毎に秘密鍵 4 によって署名されることになり、秘匿性がより一層向上する。

図 4 は、図 3 に示す電子財布 1 に格納される電子情報 3 が、さらに電子情報の発行者によって署名された情報 8 を有している構成を示す図である。電子情報 3 は、その電子情報 3 に固有の秘密鍵 4 とその証明書 5 の組と、その秘密鍵 4 によって署名された可変情報 7 と、電子情報の発行者によって署名された情報 8 とを備えて成る。秘密鍵 4 により署名された可変情報 7 のみならず、電子情報の発行者によって署名された情報 8 を有しているため、電子情報の可変情報の有効性が

それ自身で証明され、匿名性がより一層確保される。

図5は、図4に示す電子財布1において、秘密鍵4で署名された情報が可変情報としての可変属性情報であり、また、発行者によって署名された情報8が固定情報としての固定属性情報であることを示す図である。電子情報3は、その電子情報3に固有の秘密鍵4とその証明書5の組と、その秘密鍵4によって署名された可変属性情報9と、電子情報の発行者によって署名された固定属性情報10とを備えて成る。ここで、可変属性情報とは、例えば乗り物の回数券を例にとれば、1回使用するたびに持ち点が減じられる回数データが相当する。また、固定属性情報とは、同じく乗り物の回数券を例にとれば、その回数券の有効期間、使用可能経路などのデータが相当する。可変属性情報はデータの書き換えが行なわれる毎に秘密鍵4により署名されるから、可変情報の有効性がそれ自身で証明され、匿名性がより一層確保される。また、固定属性情報は電子情報の発行者によって署名されるから、これもまた属性情報の有効性がそれ自身で証明され、匿名性がより一層確保される。

なお、秘密鍵4により署名される情報として、上記情報6、可変情報7、および可変属性情報9のうちのいずれか1つを選択し、電子情報の発行者によって署名される情報として、上記情報8および固定属性情報10のうちのいずれか1つを選択することにより実現できる他の態様も本発明の目指す構成である。

また、本発明では、図5に示す電子財布1に格納される電子情報3と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された、固定属性情報と表示制御情報をさらに備え、これら3つの情報を用いて表示データを生成するようにすることもできる。

また、本発明では、図5に示す電子財布1に格納される電子情報3と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報を有するとともに、表示制御情報を取得するための情報をさらに備えることもできる。

また、本発明では、図5に示す電子財布1に格納される電子情報3と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報を有するとともに、電子情報の発行者によって署

名され或いは署名されていない表示リソースの識別情報をさらに備え、これら 3 つの情報を用いて表示データを生成するようにすることもできる。

また、本発明では、図 5 に示す電子財布 1 に格納される電子情報 3 と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報とを有するとともに、表示制御情報の識別情報及び電子情報の発行者によって署名され或いは署名されていない表示リソースを取得するための情報をさらに備えることもできる。

また、本発明では、図 5 に示す電子財布 1 に格納される電子情報 3 と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報とを有するとともに、電子情報ハンドラの認証鍵をさらに備え、前記電子情報ハンドラに、電子情報を有する端末との間で決済処理を行なわせるようにすることもできる。

また、本発明では、図 5 に示す電子財布 1 に格納される電子情報 3 と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報とを有するとともに、表示制御情報を取得するための情報と、表示リソースを取得するための情報及び電子情報ハンドラの認証鍵を備えることもできる。

また、本発明では、図 5 に示す電子財布 1 に格納される電子情報 3 と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報とを有するとともに、サービス制御情報をさらに備え、前記サービス制御情報は、電子情報により行なう決済処理を規定するようにすることもできる。

また、本発明では、図 5 に示す電子財布 1 に格納される電子情報 3 と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報とを有するとともに、表示制御情報を取得するための情報と、表示リソースを取得するための情報と、電子情報ハンドラの認証鍵及びサービス制御情報をさらに備えることもできる。

また、本発明では、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備え、前記電子情報オブジェクトが、決済処理を実行する際に、

交換する各メッセージに、前記サービス制御情報に基づく決済処理データを埋め込むようにすることが可能である。これにより、電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

また、本発明では、前記サービス制御情報が、サービス制御モジュール情報の組合せから成るようにすることができる。

また、本発明では、前記電子情報オブジェクトが、決済処理を実行する際に、決済処理に交換する各メッセージに埋め込まれるサービス制御情報に基づく決済処理メッセージが、電子情報から電子情報ハンドラに決済処理を申し出るメッセージであるようにすることができる。各種の電子情報における決済処理を、効率的に行うことが出来る。

また、本発明では、前記電子情報オブジェクトが、決済処理を実行する際に、決済処理に交換する各メッセージに埋め込まれるサービス制御情報に基づく決済処理メッセージが、電子情報ハンドラから電子情報に属性値の変更を命令するメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

また、本発明では、前記電子情報オブジェクトが、決済処理を実行する際に、決済処理に交換する各メッセージに埋め込まれるサービス制御情報に基づく決済処理メッセージが、電子情報から電子情報ハンドラに属性値の変更結果を示すメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

また、本発明では、前記電子情報オブジェクトが、決済処理を実行する際に、決済処理に交換する各メッセージに埋め込まれるサービス制御情報に基づく決済処理メッセージが、電子情報ハンドラから電子情報への領収書に相当するメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

実施例

以下、本発明の2つの実施例について、図6から図37を用いて説明する。なお、本発明はこれらの実施の形態に何ら限定されるものではなく、その趣旨を逸脱しない範囲において、種々なる態様で実施し得る。また、各図は図6、図7・

・ ・ のように表示して説明する。

実施例 1

本発明の具体的な実施例の一つであるモバイル・エレクトロニックコマース・システムは、個人消費者が、ネットワークを介して、各種のチケットや、プリペイドカードを電子情報として購入し、チケットの改札や、一般の小売販売店で商品を購入の際に、係員に対してチケットを提示したり、店員との間で、直接、現金やレシートを受け渡したりすることなく、全て、無線通信によって、チケットの改札、商品やサービスの売買決済を行なうシステムである。

以下では、本システムをモバイル・エレクトロニックコマース・システムと呼び、本システムで扱われる電子化されたチケットやプリペイドカードを電子バリュー、本システムによって提供される各種のサービスを、総称して、モバイル・エレクトロニックコマース・サービスと呼ぶこととする。

このモバイル・エレクトロニックコマース・システムは、図 6 のシステム構成図に示すように、2 系統の双方向無線通信機能とブラウザ機能と電子財布機能とを持つモバイルユーザ端末 101 と、双方向の通信機能とブラウザ機能と電子財布機能とを持つユーザ端末 107 と、電子バリューの改札決済処理を行なうサービス端末 105 と、オンライン上で電子バリューの改札決済処理を行なうサービスサーバ 106 と、銀行、クレジットサービス会社または決済処理会社における口座決済処理を行なう決済処理サーバ 104 と、オンライン上で電子バリューに関する情報提供および電子バリューの販売を行う情報提供サーバ 102 と、電子バリューを生成・発行する電子バリュー発行サーバ 103 とを備え、これらはインターネット 100 によって結ばれている。サービスサーバ 106 と決済処理サーバ 104 と情報提供サーバ 102 と電子バリュー発行サーバ 103 は、それぞれ、1 台もしくは複数台のコンピュータによって構成されるシステムである。

モバイルユーザ端末 101 は、赤外線通信とデジタル無線通信との 2 系統の双方向無線通信機能と、ブラウザ機能と電子財布機能とを持つ携帯無線電話端末である。

また、サービス端末 105 は、赤外線通信とデジタル無線通信との 2 系統の双方向無線通信機能を持ち、用途に応じて据置タイプや携帯タイプがある。

なお、図6において、108と113は、モバイルユーザ端末101とサービス端末105が、それぞれ、インターネット100にアクセスしている際に行うデジタル無線通信の伝送路を示し、109は、モバイルユーザ端末101がサービス端末105と行う赤外線通信の伝送路を示し、110、111、112、114、115は、それぞれ、サービス提供サーバ102、電子バリュー発行サーバ103、決済処理サーバ104、サービスサーバ106、ユーザ端末107がインターネット100に接続するデジタル通信回線を示している。

また、モバイル・エレクトロニックコマース・サービスの通常の運用形態としては、次のような形態を想定している。

決済処理サーバ104は、銀行またはクレジットカード会社または決済処理会社に設置され、情報提供サーバ102は、イベント会社、チケット発行会社、小売販売会社またはプリペイドカード発行会社等のオンライン上で電子バリューに関する情報の提供および電子バリューの販売を行う事業会社にそれぞれ設置される。

また、サービス端末105は、据置タイプの場合には、映画館やイベント会場等の入口、小売販売店のレジカウンタに設置され、携帯タイプの場合には、売場販売員や、集金担当者が携帯し、サービスサーバ106は、オンラインショップやインターネット放送など電子バリューに応じたサービスを提供する会社に設置される。

モバイルユーザ端末101は、消費者が持ち歩き、ユーザ端末107は、消費者が自宅に設置する。

電子バリュー発行サーバ103は、モバイル・エレクトロニックコマース・サービスを提供する会社に設置される。

さらに、モバイル・エレクトロニックコマース・システムを構成する各機器、および、各システムの所有者間の社会的な関係として、次のような関係を前提としている。

モバイルユーザ端末101の所有する消費者は、銀行またはクレジットカード会社との間で、口座決済サービスの契約を、モバイル・エレクトロニックコマース・サービスを提供する会社との間では、モバイル・エレクトロニックコマース・サービスの会員契約を結んでいる。

サービス端末 105 の所有者とサービスサーバ 106 の所有者は、モバイル・エレクトロニックコマース・サービスの提供者との間で、モバイル・エレクトロニックコマース・サービスの加盟店契約を結んでいる。但し、サービス端末 105 の所有者またはサービスサーバ 106 の所有者が、モバイル・エレクトロニックコマース・サービスの提供者と、同一の事業者であっても良い。

情報提供サーバ 106 の所有者は、モバイル・エレクトロニックコマース・サービスの提供者との間で、情報提供サーバ 106 からの要求に応じて、電子バリュー発行サーバ 103 が電子バリューを発行する契約を結んでいる。但し、情報提供サーバ 106 の所有者が、モバイル・エレクトロニックコマース・サービスの提供者と、同一の事業者であっても良い。

以下では、本システムの説明を簡単にするために、モバイルユーザ端末 101 の所有する消費者をユーザ(User)、サービス端末 105 またはサービスサーバ 106 を所有し、商品やサービスを提供・販売する事業者をマーチャント(Merchant)、電子バリュー発行サーバ 103 を所有しモバイル・エレクトロニックコマース・サービスを提供する会社をサービス提供者(Service Provider)、決済処理サーバ 104 を所有し口座決済処理を行なう銀行、クレジットカード会社または決済処理会社を決済処理機関(トランザクション Processor)、情報提供サーバ 102 を所有し、オンライン上で電子バリューに関する情報提供および電子バリューの販売を行う事業者を電子バリュー販売者(Electronic Value seller)呼ぶこととする。

本システムによって提供されるモバイル・エレクトロニックコマース・サービスは、ネットワークを介したチケットやプリペイドカードの売買と、それに伴うこれらの配送と、それらチケットやプリペイドカードの使用を、全て電子的に行なうサービスである。

具体的には、ユーザがモバイルユーザ端末 101 を用いて、インターネットを介して、情報提供サーバ 102 に電子バリューの購入オーダーをし、電子バリュー発行サーバ 103 から、情報提供サーバ 102 の電子バリュー発行要求に基づいて電子バリュー発行サーバ 103 が生成した電子バリューを受信して、それをモバイルユーザ端末 101 に蓄積して管理し、電子バリューを使用する際には、サービス端末 105 またはサービスサーバ 106 とのデータ通信によって、モバイルユーザ端末に

蓄積されている電子バリューを提示し、電子バリューの改札決済処理情報を交換して、電子バリューの改札決済処理を行い、マーチャントがサービスまたは商品の提供を行うものである。また、この時の電子バリューの売買に伴う決済処理は、情報提供サーバ 10 と決済処理サーバ 14 との間で行われる。モバイル・エレクトロニックコマース・サービスの詳細については、後で詳しく説明する。

モバイル・エレクトロニックコマース・サービスにおいて、本システムの各機器間で行われるデータ通信は、次に示す伝送路または通信回線を用いて行われる。まず、モバイルユーザ端末 101 は、伝送路 108 とインターネット 100 とデジタル通信回線 110 とを介して情報提供サーバ 102 とデジタル通信を行い、伝送路 108 とインターネット 100 とデジタル通信回線 111 とを介して電子バリュー発行サーバ 103 とデジタル通信を行い、伝送路 108 とインターネット 100 とデジタル通信回線 111 とを介してサービスサーバ 106 とデジタル通信を行い、伝送路 109 を介してサービス端末 105 と赤外線通信を行う。

また、モバイルユーザ端末 101 と電子バリュー発行サーバ 103 との通信、モバイルユーザ端末 101 とサービス端末 105 との通信、モバイルユーザ端末 101 とサービスサーバ 106 との通信では、交換される情報を、全て、暗号化して通信する。暗号化には、秘密鍵方式の暗号処理と公開鍵方式の暗号処理とを組合わせて、情報を電子封書化して通信する。

次に、本システムを構成する各構成要素について説明する。

まず、サービス端末 105 について説明する。

図 11 は、サービス端末 105 のブロック構成図である。図 11 において、サービス端末 105 は、コンピュータ 600 と無線通信モデム 601 と赤外線通信アダプタ 602 によって構成される。サービス端末 105 には、デジタル無線通信と赤外線通信の 2 系統の通信機能があり、デジタル無線通信機能によってインターネットアクセスを行い、赤外線通信機能によってモバイルユーザ端末との電子バリューの改札決済処理を行う。コンピュータ 600 には、マーチャントアプリケーションが搭載されており、このマーチャントアプリケーションに基づいて、コンピュータ 600 が無線通信モデム 601 と赤外線通信アダプタ 602 を制御して、電子バリューの改札決済処理を行う。同様に、サービスサーバ 106 にも、マーチャントアプリ

ケーションが搭載されており、サービスサーバ106は、このマーチャントアプリケーションに基づいて、電子バリューの改札決済処理を行う。改札決済処理におけるサービス端末105とサービスサーバ106の詳細な動作とについては、後で詳しく説明する。

次に、ユーザ端末107について説明する。

図12は、ユーザ端末107のブロック構成図である。図12において、ユーザ端末107は、コンピュータ700とスマートカードリーダーライタ701と通信モデム702によって構成される。ユーザ端末107には、ブラウザアプリケーションプログラムと電子財布アプリケーションプログラムが搭載されており、インターネットへのアクセスは通信モデム702によって行う。ユーザ端末107は、スマートカードリーダーライタ701に、モバイルユーザ端末101のスマートカードを挿入することにより、サービス端末105との改札決済処理を除いて、モバイルユーザ端末101と同じ機能を持つ。

次に、モバイルユーザ端末101について説明する。

図7(a)、図7(b)は、それぞれ、モバイルユーザ端末101の前面側及び背面側の外観図である。図7(a)において、211は、サービス端末105と赤外線通信を行なう赤外線通信ポート(赤外線通信モジュール)、210は、デジタル無線通信の電波を受発信するアンテナ、209は、レシーバスピーカ、200は、120×160画素表示のカラー液晶ディスプレイ(LCD)、203は、通話スイッチ、202は、通話の終了スイッチと電源スイッチを兼ねた終了/電源スイッチ、204は、ナビゲーションスイッチ、205と206はファンクションスイッチ、201は、テンキースイッチ、207は、マイクである。さらに、図7(b)において、212は、スマートカードスロット(スマートカードリーダーライタ)である。

モバイルユーザ端末101には、デジタル無線通信と赤外線通信の2系統の通信機能があり、デジタル無線通信機能によって音声通話とインターネットアクセス、及びサービスサーバとの電子バリューの改札決済処理を行い、赤外線通信機能によってサービス端末との電子バリューの改札決済処理を行う。さらに、モバイルユーザ端末101には、ブラウザ機能と電子財布機能があり、ブラウザ機能によってインターネットとモバイルユーザ端末のローカルデータのブラウジングを行い、

電子財布機能によって電子バリューの管理、及び改札決済処理を行う。

図8は、モバイルユーザ端末101のブロック構成図である。図8において、モバイルユーザ端末101は、F e R A M (Ferroelectric Random Access Memory) 301に格納されたプログラムにしたがって、F e R A M 301に格納されたデータの処理と送受信データの処理、並びにバス306を介して他の構成要素の制御を行なうC P U (中央処理装置: Central Processing Unit) 300と、L C D 200と、赤外線通信モジュール211と、スマートカードリーダライタ212と、テンキースイッチ201、終了/電源スイッチ202、通話スイッチ203、ナビゲーションスイッチ204、及びファンクションスイッチ205、206と、スイッチ操作を検出するキー制御部302と、スピーカ303とレシーバ209をドライブしマイク207から入力するアナログ音声信号をデジタル処理する音声処理部304と、アンテナ210を介して行う無線データ通信及び無線音声通信を制御する無線通信部305と、スマートカード307とによって構成される。

スマートカード307は、C P Uと不揮発性メモリを内蔵し、不揮発性メモリには、ユーザのU P T (Universal Personal Telecommunication) 番号(電話番号)と、モバイル・エレクトロニックコマース・サービスにおけるユーザI Dと、公開鍵暗号方式のユーザ秘密鍵と、それに対応するユーザ証明書、並びに、サービス提供者証明書(サービス提供者のデジタル証明書)と、ユーザが購入した電子バリューと、電子バリューの購入及び改札決済処理の領収書が格納される。

F e R A M 301には、O S (Operating System) と電話の他に、ブラウザと電子財布の2つのアプリケーションプログラムが格納されており、C P U 300は、これらのアプリケーションを同時に実行する。

図9は、C P U 300が実行するアプリケーション(ブラウザと電子財布)と、モバイルユーザ端末101の他の構成要素と、他の機器との関係を示す模式図である。図4において、C P U 300は、ブラウザ401と電子財布400の2つのプロセスを実行する。

ブラウザ401は、キー制御部302から送られるユーザ操作情報(スイッチ操作)に基づいて、無線通信部305を用いて、情報提供サーバ103とインターネット100を介して通信し、情報提供サーバ103から受信したデータを解釈して、L C

D 200 に表示する。この時、情報提供サーバ 103 から受信するデータは、特定のマークアップ記述言語に基づいて記述されており、ブラウザ 401 は、このマークアップ記述言語を解釈して画像データを生成し、LCD 200 に表示する。また同様に、ブラウザ 401 は、FeRAM 301 に格納されたファイルや、電子財布 400 から受信したデータを解釈し、LCD 200 に表示する。この時、FeRAM 301 に格納されたファイル、及び電子財布 400 から受信したデータは、特定のマークアップ記述言語に基づいて記述されている。

例えば、図 10 (a) は、電源をオンした時に LCD 200 に表示されるマイメニュー画面を示している。終了／電源スイッチ 202 によって電源をオンすると、ブラウザ 401 は、まず、FeRAM 301 に格納されたマイメニューファイルを読み出し、図 10 (a) に示す画面を表示する。マイメニューファイルは、モバイルユーザ端末 101 の操作メニューであり、特定のマークアップ記述言語に基づいて記述されている。

ここで例えば、"1 Internet"を選択すると、ブラウザ 401 は、インターネットにアクセスし、"1 Internet"にリンクされた図 10 (b) に示すインターネットメニュー画面を表示する。ユーザは、このインターネットメニュー画面からインターネット上のサイト、例えば情報提供サーバ 102 にアクセスをする。図 10 (c) は、情報提供サーバ 102 にアクセスし、電子バリューをオーダーする場合の画面の一例を示している。

また、"2 E-Wallet"を選択すると、ブラウザ 401 は、電子財布 400 にアクセスし、電子財布 400 から受信したデータに基づいて、図 10 (d) に示すパスワードの入力を要求する画面を表示する。さらにこの画面でパスワードを入力すると、ブラウザ 401 は、入力されたパスワードを電子財布 400 に送信し、パスワードが正しい場合、電子財布 400 からブラウザ 401 に、電子財布 400 で管理されている電子バリューの一覧を示すデータが送信され、ブラウザ 401 は、図 10 (e) に示す画面を表示する。パスワードが間違っている場合には、エラー画面が表示される。さらに、"7 Soccer 200X Japa"を選択すると、電子財布 400 からブラウザ 401 に、選択された電子バリューの内容を示すデータが送信され、ブラウザ 401 は、図 10 (f) に示す画面を表示する。以上において、電子財布 400 からブラ

ウザ 401 に送信されるデータは、特定のマークアップ記述言語に基づいて記述されている。

図 10 (a) ~ (f) に示すように、ブラウザ 401 が LCD 200 に表示する画面は、受信したデータを表示するコンテンツ表示領域 500 と、画面上部の状態表示領域 502 と、画面下部のメニュー表示領域 502 の 3 つの領域に分けられる。状態表示領域 502 には、現在、どこと通信しているか、及び通信がセキュアか否かが示される。例えば、図 10 (c) の場合には、表示されている画面がインターネットをアクセスしたもので、その通信がセキュアな通信で盗聴されないことを示している。また、図 10 (e) の場合には、表示されている画面が電子財布 400 をアクセスしたもので、ブラウザ 401 と電子財布 400 間の通信がセキュアな通信で盗聴されないことを示している。

メニュー表示領域 502 は、表示中の画面において、ファンクションスイッチ 205、206 に割り当てられたファンクションを示す領域である。例えば、図 10 (a) の場合には、ファンクションスイッチ 205 に "ok" つまり「選択」を意味するファンクションが割り当てられ、ファンクションスイッチ 206 に "back" つまり「戻る」を意味するファンクションが割り当てられる。

一方、電子財布 400 は、ブラウザ 401 からの要求に応じて、電子バリュー発行サーバ 103 からの電子バリューの受信と、スマートカード 307 に格納された電子バリューの管理、及びサービス端末 105 またはサービスサーバ 106 との改札決済処理を行う。

例えば、図 10 (a) のマイメニュー画面で、ユーザが "2 E-Wallet" を選択した場合、"2 E-Wallet" には、"wallet:///index" という URI (Uniform Resource Identifier) がリンクされており、ブラウザ 401 は電子財布 400 に電子財布内のインテックス情報つまり電子財布 400 で管理されている電子バリューの一覧を要求する。それに対し、電子財布 400 は、特定のマークアップ記述言語で記述されたパスワード入力画面データをブラウザ 401 に返し、次にブラウザからユーザが入力したパスワードが送信されると、スマートカードリーダライタ 212 を介してスマートカード 307 にアクセスし、スマートカード 307 に登録されたパスワードと照合してパスワードが正しい場合に、つまりユーザが認証された場合に、特

定のマークアップ記述言語で記述されたスマートカード 307 に格納されている電子バリューの一覧を示すデータをブラウザ 401 に返す。

さらに、図 10 (e) の電子バリューの一覧画面で、ユーザが”7 Soccer 200X Japa”を選択した場合、”7 Soccer 200X Japa”に、”wallet:///Evalue/ev00000033”という U R I がリンクされており、ブラウザ 401 は電子財布 400 に”ev00000033”という識別子で管理されている電子バリューを要求する。それに対し、電子財布 400 は、スマートカードリーダーライタ 212 を介してスマートカード 307 にアクセスし、スマートカード 307 の不揮発性メモリに”ev00000033”という識別子で格納管理されている電子バリューデータから、電子バリューオブジェクトを生成し、さらに、生成した電子バリューオブジェクトに電子バリューの内容を示すデータを要求し、電子バリューオブジェクトが生成した電子バリューの内容を示すデータを、ブラウザ 401 に返す。この時、電子バリューオブジェクトが生成する電子バリューの内容を示すデータは、特定のマークアップ記述言語に基づいて記述されている。

また例えば、電子バリューの購入の場合には、電子財布 400 は、ブラウザ 401 からの電子バリューの受信要求に基づいて、電子バリュー発行サーバ 103 からの電子バリューを受信する。

ブラウザ 401 による情報提供サーバ 102 への電子バリューの購入オーダーに対して、情報提供サーバ 102 は、電子バリュー発行サーバ 103 に電子バリュー発行要求を送信し、電子バリュー発行サーバ 103 から電子バリューを受信するためのセッション番号を取得して、ユーザに電子バリューの受信操作を促すデータをブラウザ 401 に対して送信する。図 26 は、この時に情報提供サーバ 102 からブラウザ 401 に送信される電子バリューの受信操作を促すデータの一例を示し、図 10 (g) は、ブラウザ 401 が、このデータを表示した画面を示している。ユーザが”Receive e-Value”を選択すると、<Go HREF=”wallet:///evReceive”>が実行され、ブラウザ 401 から電子財布 400 に電子バリューの受信が要求される。この時、パラメータとして、電子バリュー発行サーバ 103 の U R I (EV_ISSUER_URI=”http://www.evalue.com”)と、電子バリューを受信するためのセッション番号 (SESSION_NUM=”a01b23c45d67e89f”)とが、ブラウザ 401 か

ら電子財布 400 に送られる。

ブラウザ 401 から電子バリューの受信を要求された電子財布 400 は、無線通信部 305 を介して電子バリュー発行サーバ 103 (EV_ISSUER_URI="http://www.evalue.com") にアクセスし、スマートカード 307 に格納されているユーザ秘密鍵とユーザ証明書とサービス提供者証明書を用いて、電子バリュー発行サーバ 103 との間で相互認証を行い暗号化通信セッションを確立して、電子バリュー発行サーバ 103 に電子バリューの発行を要求し、電子バリュー発行サーバ 103 から電子バリューを含むデータを受信する。この時、電子財布から電子バリュー発行サーバに送信される電子バリューの発行要求には、電子財布が受信する電子バリューを示すセッション番号が含まれる。電子バリューを含むデータを受信した電子財布 400 は、受信したデータから電子バリューオブジェクトを生成し、さらに、生成した電子バリューオブジェクトに電子バリューデータの生成を要求し、電子バリューオブジェクトが生成した電子バリューデータをスマートカード 307 に格納して、電子バリューを電子財布に登録する。ここで電子バリューデータとは、電子バリューオブジェクトを特定のフォーマットのシリアルデータに変換したものであり、また、そのシリアルデータへの変換処理には、暗号化処理が含まれていても良い。

また、電子バリューの改札決済処理の場合には、電子財布 400 は、ブラウザ 401 からの電子バリューの改札決済処理要求に基づいて、サービス端末 105 またはサービスサーバ 106 との間で改札決済処理を行う。ブラウザ 401 からの改札決済処理要求に対し、ブラウザ 401 がサービスサーバ 106 と通信中の場合には、電子財布 400 は無線通信部 305 を介してサービスサーバ 106 と改札決済処理を行い、ブラウザ 401 がサービスサーバ 106 と通信していない場合には、電子財布 400 は赤外線通信モジュール 211 を介してサービス端末 105 と改札決済処理を行う。電子バリューの改札決済処理については後で詳しく説明する。

次に、スマートカード 307 に格納される電子バリュー (電子バリューデータ) のデータ構造について説明する。図 13 は、電子バリューのデータ構造を示す模式図である。図 13 において、一つの電子バリューは、バリュー属性記述部 800、サービス制御部 803、セキュリティ情報部 804、表示制御部 805、表示リソース

部 806 の 5 つの部分から構成される。

バリュー属性記述部 800 は、電子バリューのタイプ、コード番号、ID 番号、名称など、各種属性を規定する部分で、バリュー属性記述部 800 は、さらに、改札決済処理により値が変化しない固定属性を示すプレゼンテーションカード 801 と、改札決済処理により値が変化する可変属性 802 に分けられる。サービス制御部 803 は、電子バリューが改札決済処理で行う処理の内容を規定する部分であり、セキュリティ情報部 804 は、電子バリューが持つ暗号鍵等の機密情報を規定する部分、表示制御部 805 は、電子バリューの表示を規定する部分、表示リソース部 806 は、電子バリューの表示及びサウンド効果に用いるイメージデータや音声データ等を規定する部分である。

また、電子バリューのデータ構造は、特定のマークアップ記述言語に基づいており、スマートカード 307 には、それをさらにエンコードしたものが格納される。図 17 は、特定のマークアップ記述言語で記述された電子バリューの一例を、一部省略して示しており、この場合、この電子バリューは、電子財布 400 に "ev00000033" という識別子で管理されている。

プレゼンテーションカード 801 は、サービス提供者 (<http://www.evalue.com>) によりデジタル署名されており、可変属性 802 は、この電子バリューの秘密鍵 (evPrivateKey) によって、つまり、この電子バリュー自身によってデジタル署名されている。また、サービス制御部 803 とセキュリティ情報部 804 と表示制御部 805 と表示リソース部 806 は、サービス提供者 (<http://www.evalue.com>) によりデジタル署名されている。これらのデジタル署名は、電子バリューオブジェクトが生成される度に検証される為、これらの部分に不正な改竄をすることは難しい。ただし、表示制御部 805 と表示リソース部 806 は、その URI のみ規定されており、表示制御部の実体は、1201 の部分で、表示リソース部の実体は、1202 の部分で、それぞれ個別に規定される。または、サービス提供者 (<http://www.evalue.com>) についても、1200 の部分で規定される。

図 18 は、図 17 に示した電子バリューのプレゼンテーションカード 801 と可変属性 802 を省略無しに示したものである。図 18 によれば、この電子バリューには、固定属性として、電子バリューのタイプ (evType) がチケット (ticket) で、

[illegible]

図19は、図17に示した電子バリューのサービス制御部803とセキュリティ情報部804を省略無しに示したものである。図19によれば、この電子バリューには、チケットモジュール(ticket)と属性検証モジュール(verify_prop)とメッセージ設定モジュール(set_message)の3つのサービス制御モジュールが規定されている。ここで、サービス制御モジュールとは、改札決済処理で行う処理を、小さな処理モジュールに部品化したものである。改札決済処理では、サービス制御部803に規定されたサービス制御モジュールがそれぞれ実行される。つまり、サービス制御部803に規定するサービス制御モジュールの組合わせを変えることによって、各種の改札決済処理を規定することが出来る。

例えば、この電子バリューの場合、チケットモジュールは、チケットの基本機能をモジュール化したものであり、改札決済処理によって、チケットの回数券枚数(\$NUMBER)を”1”デクリメントし、有効期間の開始日時(\$START_VALID)と終了日時(\$END_VALID)をそれぞれ設定し、使用済フラグ(\$USED)を”1”（つまり使用済）に、有効性フラグ(\$VALIDITY)を有効期間に応じて設定し、電子バリューを使用した回数、つまり改札決済処理の回数を示す使用シリアル番号(\$USE_SERIAL)を”1”インクリメントする。属性検証モジュールは、指定された電子バリューの属性を検証するモジュールであり、この場合、改札決済処理によって席番号(\$SEAT_NUMBER)が検証される。メッセージ設定モジュールは、メッセージ（文字列）を設定するモジュールであり、改札決済処理によって、可変属性の1つであるメッセージ2(\$MESSAGE_2)に、サービス端末105（または、サービスサーバ106）に設定されたメッセージが設定される。以上の処理が、1回の改札決済処理の中で、同時に行われる。

また、セキュリティ情報部 804 には、この電子バリュウー固有の鍵である公開鍵

暗号方式の電子バリュー秘密鍵(evPrivateKey)と、それに対応する電子バリュー証明書(evCertificate)、並びに、電子バリューのコード番号毎に固有の鍵である共通鍵方式の電子バリュー認証鍵(evAuthKey)と電子バリューハンドラ認証鍵(evhandlerAuthKey)等が規定されている。ここで、電子バリューハンドラとは、この電子バリューと改札決済処理を行うサービス端末 105 またはサービスサーバ 106 に、予め設定されている改札決済処理のための情報である。サービス端末 105 またはサービスサーバ 106 では、改札決済処理時に、この情報から電子バリューハンドラオブジェクトが生成され、実質的に、電子バリューオブジェクトと電子バリューハンドラオブジェクトとの間で改札決済処理が行われる。電子バリューハンドラについては、後で詳しく説明する。

図 20 は、図 17 に示した電子バリューの表示制御部の実体 1201 を省略無しに示したものである。図 20 によれば、この電子バリューには、“Main”と“Detail”の 2 つの画面情報が規定されている。表示制御部の実体 1201 には、マークアップ記述言語による表示画面のテンプレートが規定されている。この電子バリューの電子バリューオブジェクトは、`<evP>`と`</evP>`に挟まれた部分をプレゼンテーションカード 801 で規定されている属性の値に、`<evV>`と`</evV>`に挟まれた部分を可変属性 802 で規定されている属性の値に、それぞれ置きかえることによって、電子バリューの内容を示すデータを生成する。例えば、図 10 (e) の電子バリューの一覧画面で、ユーザが“7 Soccer 200X Japa”を選択した場合には、電子バリューオブジェクトは、図 22 に示す“Main”の画面情報を生成し、ブラウザ 401 によって、LCD200 には、図 10 (f) に示す画面が表示される。

図 21 は、図 17 に示した電子バリューの表示リソース部の実体 1202 を詳細に示したものである。図 21 によれば、この電子バリューには、“MAIN_IMG”と“MAP”というラベルが付けられた 2 つのイメージデータと、“Greet”というラベルが付けられた 1 つの音声データが規定されている。

例えば、図 22 に示した“Main”の画面情報の場合、“`<IMGSRC=wallet:///evResource label=MAIN_IMG>`”の部分は、電子財布 400 に存在する電子バリューオブジェクトの表示リソース部の中のラベルが“MAIN_IMG”のイメージの表示を規定している記述であり、図 21 に示したリソースデータの内、“MAIN_IMG”というラベ

ルが付いたイメージデータが、ブラウザ 401 に送られ、図 10 (f) に示すような画面が表示される。

このように、一つの電子バリューが持つ各種の属性、改札決済処理で行う処理の内容、及び電子バリューの表示は、このようなマークアップ記述言語に基づいて規定される。

なお、電子バリューの表示制御部の実体 1201 と表示リソース部の実体 1202 は、スマートカード 307 に格納せずに、F e R A M 301 に格納しするようにしても良い。この場合、スマートカード 307 に格納する電子バリュー一つ当たりの容量を小さく出来るので、スマートカード 307 に、より多くの電子バリューを格納することが出来るというメリットがある。また、スマートカード 307 に比べ F e R A M 301 には容量に余裕があるので、容量の大きい表示制御部の実体 1201 と表示リソース部の実体 1202 を持つ電子バリューをモバイルユーザ端末 101 で取り扱うことができる。つまり、表示制御部として、スクリプト等を用いた電子バリューの複雑な表示が規定された電子バリューや、表示リソース部として、カラー画像などのマルチメディア情報が設定された電子バリュー等の多彩な表現力を持った電子バリューを扱うことができる。

ただしこの場合、ユーザ端末 107 のスマートカードリーダーライタ 701 にスマートカード 307 を挿入して、コンピュータ 700 の画面に電子バリューの内容を表示する際、表示制御部の実体 1201 と表示リソース部の実体 1202 が必要になるが、表示制御部 805 と表示リソース部 806 に規定されているそれらの実体の U R I を基に、インターネット 100 を介して表示制御部の実体 1201 と表示リソース部の実体 1202 をダウンロードすることにより、電子バリューの内容を表示することが出来る。また、この時、ユーザ端末 107 の種類と画面サイズに合った表示制御部の実体 1201 と表示リソース部の実体 1202 とがダウンロードされる。つまり、ユーザ端末 107 に表示される電子バリューは、モバイルユーザ端末 101 の小さな表示画面を想定したものとは異なり、ユーザ端末 107 の画面サイズにあった多彩な表現力を持った電子バリューが表示される。

この端末に応じた表示制御部の実体 1201 と表示リソース部の実体 1202 のダウンロードの仕組みについては、後で詳しく説明する。

次に、電子バリューハンドラについて説明する。電子バリューハンドラは、電子バリューのコード番号に対応して存在し、サービス提供者によって、予め、その電子バリューを取り扱うマーチャントのサービス端末 105 及びサービスサーバ 106 に対して、インターネット 100 を介して配布されている。

図 1 4 は、電子バリューハンドラのデータ構造を示す模式図である。図 1 4 において、一つの電子バリューハンドラは、バリュー属性記述部 900、サービス制御部 903、セキュリティ情報部 904 とマーチャントオプション 905 の 4 つの部分から構成される。バリュー属性記述部 900 は、取り扱う電子バリューのタイプ、コード番号、ID 番号、名称など、各種属性を規定する部分であり、サービス制御部 903 は、電子バリューとの改札決済処理で行う処理の内容を規定する部分であり、セキュリティ情報部 904 は、電子バリューハンドラが持つ暗号鍵等の機密情報を規定する部分、マーチャントオプション 905 は、マーチャント独自の追加設定を規定する部分である。

電子バリューハンドラもまた、そのデータ構造は、特定のマークアップ記述言語に基づいており、サービス端末 105 またはサービスサーバ 106 には、それをさらにエンコードしたものが格納される。

図 2 3 は、図 1 7 に示した電子バリューに対応する電子バリューハンドラのマークアップ記述言語による記述を一部省略して示しており、この場合、この電子バリューハンドラは、電子マーチャントに“ev00000001”という識別子で管理されている。電子バリューハンドラを構成するデータの内、バリュー属性記述部 900 とサービス制御部 903 とセキュリティ情報部 904 がサービス提供者から配布されたものであり、マーチャントオプション 905 は、マーチャントがマーチャントアプリケーションによって追加設定したものである。したがって、バリュー属性記述部 900 とサービス制御部 903 とセキュリティ情報部 904 の部分にのみ、サービス提供者 (<http://www.evalue.com>) によるデジタル署名が施されている。このデジタル署名は、電子バリューハンドラオブジェクトが生成される度に検証される為、これらの部分に不正な改竄をすることは難しい。

図 2 3 のバリュー属性記述部 900 によれば、取り扱う電子バリューは、電子バリューのタイプ(evType)がチケット(ticket)で、コード番号(evCode)が“0000300

000000201”、チケットのタイトル(TITLE)が、” Soccer 200X Japan vs Brazil” といった属性を持っている。ただし、席番号(SEAT_NUM)とメッセージ2 (MESSAGE_2)に関しては規定されておらず、それぞれには、電子バリューハンドラの所有者（マーチャント）による設定を許可する permission=”public”という要素が付加されている。これにより、マーチャントによるマーチャントオプション 905 の追加が可能になり、例えば、図 2 3 のマーチャントオプション 905 では、席番号 (\$SEAT_NUM)に”SS-*-*”が、メッセージ2 (\$MESSAGE_2)に” Special News available: <http://www.yis.co.jp/news/20020630>”がそれぞれ設定されている。

図 2 3 のサービス制御部 903 には、電子バリューのチケットモジュール(ticket)と属性検証モジュール(verify_prop)とメッセージ設定モジュール(set_message)に対応するサービスモジュールが規定されている。マークアップ記述言語による記述は電子バリューと同じであるが、それぞれ、マーチャント側の処理を行うサービスモジュールが実行される。例えば、属性検証モジュールの場合には、マーチャントオプション 905 の設定にしたがって、席番号(\$SEAT_NUM)が、”SS-*-*”と照合される。この時、'*'は任意の文字列を意味し、SS 席のチケットのみ、改札決済処理が可能となる。また、メッセージ設定モジュールの場合には、マーチャントオプション 905 の設定にしたがって、改札決済処理により、電子バリュー側のメッセージ2 (\$MESSAGE_2)に” Special News available: <http://www.yis.co.jp/news/20020630>”というメッセージが設定される。

図 2 3 のセキュリティ情報部 904 には、図 1 7 に示した電子バリューのセキュリティ情報部 804 に規定されているものと同じ電子バリュー認証鍵(evAuthKey)と電子バリューハンドラ認証鍵(evhandlerAuthKey)が規定されている。電子バリューと電子バリューハンドラは、改札決済処理の際、この電子バリュー認証鍵(evAuthKey)と電子バリューハンドラ認証鍵(evhandlerAuthKey)を用いて相互認証を行う。

次に、モバイルユーザ端末 101 とサービス端末 105 間の改札決済処理について説明する。改札決済処理は、ユーザが使用する電子バリューをLCD 200 に表示し、赤外線通信ポート（赤外線通信モジュール）をサービス端末 105 の赤外線通信アダプタ 602 に向けて、改札決済処理の実行に割り付けられたファンクションス

イッチを押すことによって開始する。例えば、図 2 2 に示した“Main”の画面の場合、改札決済処理の実行に割り付けられたファンクションスイッチを押すことによって、`<Go HREF="wallet:///evTransact"/>`が実行され、電子財布 400 上の電子バリューオブジェクトに改札決済処理が要求される。図 1 5 は、改札決済処理においてモバイルユーザ端末 101 とサービス端末 105 間で交換されるメッセージを示している。まず、電子バリューオブジェクトから電子バリューの改札決済処理を申し出るメッセージプレゼンテーション（プレゼンテーション）1003 が送信される。それに対し、サービス端末 105 のマーチャントアプリケーションは、電子バリューに対応する電子バリューハンドラオブジェクトを生成し、生成された電子バリューハンドラオブジェクトから電子バリューに属性の値の変更を要求するメッセージであるインストラクション 1004 が送信される。電子バリューオブジェクトは、インストラクション 1004 に基づいて属性の値を変更し、その変更を証明するメッセージであるトランザクション(Transaction)1005 を電子バリューハンドラオブジェクトに送信する。電子バリューハンドラオブジェクトは、トランザクション 1005 の内容を検証し、正しい場合に、トランザクション 1005 の領収書に相当するレシート (Receipt) 1006 を送信する。さらに、電子バリューオブジェクトは、レシート 1 0 0 6 の内容を検証し、正しい場合に、レシート 1 0 0 6 の受け取りを確認するメッセージであるアクノーリッジ（アクノーリッジ）1007 を電子バリューハンドラオブジェクトに送信し、属性の値が変更された電子バリューデータと Receipt をスマートカード 307 に保存して改札決済処理を終了する。改札決済処理の途中で、エラーが発生した場合には、相手側にエラーメッセージを送信して改札決済処理を中止する。

プレゼンテーション 1003 は、図 1 6 (a) に示すように、メッセージのヘッダ 1110 と、この改札決済処理を電子財布 400 からみてユニークに示す要求番号 1111 と、電子バリューのプレゼンテーションカード 1012(801)と、サービス制御モジュールによるサービス制御メッセージ 1113 に、電子バリュー秘密鍵による電子バリュー署名 1114 をし、さらに電子バリュー証明書 1115 を付加して、これを電子バリューハンドラ認証鍵で暗号化して、さらにメッセージのヘッダ 1117 と電子バリューのコード番号 1118 を付加したものである。

サービス端末 105 のマーチャントアプリケーションは、プレゼンテーション 1003 のコード番号 1118 に基づいて、電子バリューに対応する電子バリューハンドラオブジェクトを生成し、生成された電子バリューハンドラオブジェクトは、まず、電子バリューハンドラ認証鍵によって暗号化されている部分 1116 を復号化し、電子バリュー証明書 1115 さらには電子バリュー署名 1114 を検証して、サービス制御メッセージ 1113 を検証する。プレゼンテーション 1003 の検証結果が正しい場合に、電子バリューハンドラオブジェクトはインストラクション 1004 を生成、送信する。

インストラクション 1004 は、図 16 (b) に示すように、メッセージのヘッダ 1120 と、プレゼンテーション 1003 に含まれていた要求番号 1121 (1111) と、この改札決済処理をマーチャントアプリケーションからみてユニークに示す決済番号 1112 と、サービス制御モジュールによるサービス制御メッセージ 1123 に、マーチャント秘密鍵によるマーチャント署名 1124 をし、さらにマーチャント証明書 1825 と、新たに生成したセッション鍵 A 1126 を付加して、これを電子バリュー認証鍵で暗号化して、さらにメッセージのヘッダ 1128 を付加したものである。電子バリューオブジェクトは、まず、電子バリュー認証鍵によって暗号化されている部分 1127 を復号化し、電子マーチャント証明書 1125 さらにはマーチャント署名 1124 を検証して、要求番号 1111 を照合し、サービス制御メッセージ 1113 を検証する。インストラクション 1004 の検証結果が正しい場合、はじめて、電子バリューハンドラオブジェクトが正しい電子バリュー認証鍵と電子バリューハンドラ認証鍵とを持つ正当な電子バリューハンドラオブジェクトであると判定し、電子バリューオブジェクトは、インストラクション 1004 に基づいて属性の値を変更し、トランザクション 1005 を生成、送信する。

トランザクション 1005 は、図 16 (c) に示すように、メッセージのヘッダ 1130 と、要求番号 1131 と、インストラクション 1004 に含まれていた決済番号 1132 (1122) と、トランザクション 1005 の宛先に相当するマーチャント ID 1133 と、サービス制御モジュールによるサービス制御メッセージ 1134 に、電子バリュー秘密鍵による電子バリュー署名 1135 をし、新たに生成したセッション鍵 B 1136 を付加して、これをインストラクション 1004 に含まれていたセッション鍵

A1126 で暗号化して、さらにメッセージのヘッダ 1138 を付加したものである。

電子バリューハンドラオブジェクトは、まず、セッション鍵 A1126 によって暗号化されている部分 1137 を復号化し、電子バリュー署名 1135 を検証して、要求番号 1111 及び決済番号 1132 を照合し、サービス制御メッセージ 1113 を検証する。トランザクション 1005 の検証結果が正しい場合、はじめて、電子バリューオブジェクトが正しい電子バリュー認証鍵と電子バリューハンドラ認証鍵とを持つ正当な電子バリューオブジェクトであると判定し、電子バリューハンドラオブジェクトは、トランザクション 1005 の領収書に相当するレシート 1006 を生成、送信する。

レシート 1006 は、図 16 (d) に示すように、メッセージのヘッダ 1140 と、要求番号 1141 (1131) と、決済番号 1142 (1132) と、レシート 1006 の宛先に相当する電子バリュー ID 1143 と、サービス制御モジュールによるサービス制御メッセージ 1144 と、領収書情報 1145 とに、マーチャント秘密鍵によるマーチャント署名 1146 をし、さらに、トランザクション 1005 に含まれていたセッション鍵 B1136 で暗号化して、さらにメッセージのヘッダ 1148 を付加したものである。

電子バリューオブジェクトは、まず、セッション鍵 B1136 によって暗号化されている部分 1147 を復号化し、マーチャント署名 1146 を検証して、要求番号 1111 及び決済番号 1132 を照合し、サービス制御メッセージ 1113 を検証する。シート 1006 の検証結果が正しい場合、電子バリューオブジェクトは、が正しい電子バリュー認証鍵と電子バリューハンドラ認証鍵とを持つ正当な電子バリューオブジェクトであると判定し、電子バリューハンドラオブジェクトは、レシート 1006 のアクノーリッジに相当するアクノーリッジ 1007 を生成、送信する。

アクノーリッジ 1007 は、図 16 (e) に示すように、メッセージのヘッダ 1150 に、レシート 1006 に対する電子バリュー秘密鍵による電子バリュー署名 1151 を付加したものである。

電子バリューハンドラオブジェクトは、電子バリュー署名 1151 を検証して、正しい場合に、復号化されたトランザクションと Receipt を保存して改札決済処理を終了する。

一方、アクノーリッジ 1007 を送信した電子バリューオブジェクトは、属性の値を変更した電子バリューデータと、復号化された Receipt をスマートカード 307 に保存して改札決済処理を終了する。この際、電子バリューの可変属性 802 には、電子バリュー秘密鍵によって新たにデジタル署名が施される。

また、この改札決済処理において、プレゼンテーション 1003 とインストラクション 1004 とトランザクション 1005 とレシート 1006 の各メッセージに設定されるサービス制御メッセージによって、各電子バリューに固有の改札決済処理が行われる。サービス制御メッセージは、サービス制御モジュールによって設定され、相手側のサービス制御モジュールによって検証される。

プレゼンテーション 1003 とインストラクション 1004 とトランザクション 1005 とレシート 1006 には、それぞれ、図 24 (a)、(b)、(c)、(d) に示すデータをエンコードしたものが、サービス制御メッセージとして設定される。例えば、図 24 (a) の場合、電子バリューハンドラオブジェクト側の ID が "1" のサービス制御モジュール (チケットモジュール) に対し number=1 start="1999.07.23T00:00+0900" end="2002.06.30T23:59+0900" used_flag=0 validity_flag=1 serial=0、ID が "2" のサービス制御モジュール (属性検証モジュール) に対し prop=SS-A-28、ID が "3" のサービス制御モジュール (メッセージ設定モジュール) に対し msg=というように、現状の電子チケットの属性が提示され、電子バリューハンドラオブジェクトのそれぞれのサービス制御モジュールにおいて検証される。例えばこの時、電子バリューハンドラが図 23 に示したもので、prop=S-A-28 であった場合には、照合エラーとる。

図 24 (b) の場合、電子バリューオブジェクト側の ID が "1" のサービス制御モジュール (チケットモジュール) に対し number=0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+0900" used_flag=1 validity_flag=1 serial=1、ID が "3" のサービス制御モジュール (メッセージ設定モジュール) に対し msg="Special News available: <http://www.yis.co.jp/news/20020630>" というように、属性の変更命令が提示され、電子バリューオブジェクトのそれぞれのサービス制御モジュールにおいて属性が変更される。

図 24 (c) の場合、電子バリューハンドラオブジェクト側の ID が "1" のサ

ービス制御モジュール（チケットモジュール）に対し number=0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+0900" used_flag=1 validity_flag=1 serial=1、IDが"2"のサービス制御モジュール（属性検証モジュール）に対し prop=SS-A-28、IDが"3"のサービス制御モジュール（メッセージ設定モジュール）に対し msg="Special News available: <http://www.yis.co.jp/news/20020630>" というように、変更後の電子チケットの属性が提示され、電子バリューハンドラオブジェクトのそれぞれのサービス制御モジュールにおいて検証される。

図24（d）の場合、電子バリューオブジェクト側のIDが"1"のサービス制御モジュール（チケットモジュール）に対し serial=1 というように、トランザクション1005の使用シリアル番号が提示され、電子バリューオブジェクトのチケットモジュールにおいて使用シリアル番号の照合が行われる。

以上のようにして行われる改札決済処理の結果、例えば、図17に示した電子バリューの場合、可変属性は図25に示すようになる。特にこの場合、改札決済処理の結果、MESSAGE_2には、"Special News available:<http://www.yis.co.jp/news/20020630>" というマーチャントが設定したメッセージが設定され、このメッセージは電子バリューの"Detail"画面表示においてLCD200に表示される。

また、モバイルユーザ端末101とサービスサーバ106間の改札決済処理は、赤外線通信がデジタル無線通信になる以外はモバイルユーザ端末101とサービス端末105間の改札決済処理の場合と同様の手順で行われる。また、ユーザ端末107とサービスサーバ106間の改札決済処理も、通信回線115とインターネット100とデジタル通信回線114とを介して、モバイルユーザ端末101とサービス端末105間の改札決済処理の場合と同様の手順で行われる。

以上のように、モバイルユーザ端末101とサービス端末105、及び電子バリューと電子バリューハンドラを構成することにより、各種の改札決済処理、つまり各種の電子バリューを規定することができ、また、安全性を確保しつつ、マーチャントの運用におけるある程度の自由な設定を可能に出来る。

次に、電子バリュー発行サーバ103と電子バリューの発行の手順について説明する。

図27は、電子バリュー発行サーバ103のブロック構成図である。図27にお

いて、電子バリュー発行サーバ 103 は、発行する電子バリューの元データである電子バリューテンプレートデータを管理する電子バリューテンプレートデータベース 2202 と、生成した電子バリューを管理する電子バリューデータベース 2203 と、モバイル・エレクトロニックコマース・サービスの利用者であるユーザを管理するユーザデータベース 2204 と、これら電子バリューテンプレートデータベース 2202、電子バリューデータベース 2203、ユーザデータベース 2204 と通信をして電子バリューを生成する電子バリューマネージャ 2201 によって構成される。

電子バリューテンプレートデータベース 2202 には、電子バリューの種類を示す電子バリューコード (evCode) ごとに、電子バリューテンプレートが管理されている。図 28 は、電子バリューテンプレートデータベース 2202 に管理されている一つの電子バリューテンプレートデータ 2300 の構成を示している。

図 28 において、電子バリューテンプレートデータ 2300 は、電子バリューテンプレート 2301 と表示制御リスト 2302 と表示制御部生成ルール 2303 と表示リソースリスト 2304 と表示リソース部生成ルール 2305 によって構成される。電子バリューテンプレート 2301 は、特定のマークアップ記述言語で記述された発行する電子バリューの雛型であり、表示制御リスト 2302 は、発行する電子バリューに適用可能なマークアップ記述言語で記述された表示制御情報のリスト、表示制御部生成ルール 2303 は、表示制御リスト 2302 からモバイルユーザ端末（またはユーザ端末）に応じた表示制御部を選択して電子バリューの表示制御部を生成するスクリプトプログラム、表示リソースリスト 2304 は、発行する電子バリューに適用可能なイメージデータや音声データのリスト、表示リソース部生成ルール 2305 は、表示リソースリスト 2304 からモバイルユーザ端末（またはユーザ端末）に応じたイメージデータや音声データを選択して電子バリューの表示リソース部を生成するスクリプトプログラムである。表示制御リスト 2302 には、モバイルユーザ端末（またはユーザ端末）の各機種に対応した表示制御情報が含まれており、表示リソースリスト 2304 には、モバイルユーザ端末（またはユーザ端末）の各機種に対応して、同じイメージであっても解像度や色数やデータフォーマットが異なるイメージデータが含まれており、同じ音声であってもサンプリング周波数やデータフォーマットが異なる音声データが含まれている。

このように、電子バリューテンプレートデータ 2300 を構成することにより、電子バリュー発行サーバ 103 は、モバイルユーザ端末（またはユーザ端末）の種類に応じた電子バリューを発行することができる。

図 29（a）は、電子バリューの発行の手順を示している。

まず、モバイルユーザ端末 101（ブラウザ 401）からの情報提供サーバ 102 への電子バリューの購入オーダー(2401)に対して、情報提供サーバ 102 は、電子バリュー発行サーバ 103 に電子バリュー発行要求(2402)を送信する。図 30（a）は電子バリュー発行要求(2402)の一例を示しており、電子バリュー発行要求(2402)には、電子バリュータイプ(evType)や電子バリューコード(evCode)などの発行する電子バリューを規定する情報が含まれている。例えば、図 30（a）に示した電子バリュー発行要求(2402)の場合には、電子バリュータイプ(evType)が、“ticket”、電子バリューコード(evCode)が“0000300000000201”であり、電子バリュー属性情報の内の座席番号(SEAT_NUM)が“SS-A-28”、座席位置(SEAT_POS)が“<http://www.mts.com/ticket123/seat/SS-A-28>”の電子バリューを発行を要求している。

電子バリュー発行要求(2401)を受信した電子バリュー発行サーバ 103 は、要求された電子バリューが発行可能な場合、ユーザが電子バリューを受信するためのセッション番号(2403)を情報提供サーバ 102 に送信し、セッション番号(2403)を受信した情報提供サーバ 102 は、ユーザに電子バリューの受信操作を促す電子バリュー受信操作画面データ(2404)をモバイルユーザ端末 101（ブラウザ 401）に対して送信する。電子バリュー受信操作画面データ(2404)を受信したモバイルユーザ端末 101（ブラウザ 401）は、図 10（g）に示すような画面を表示する。

図 26 は、この電子バリュー受信操作画面データ(2404)の一例を示しており、電子バリュー受信操作画面データ(2404)には、ユーザが電子バリュー発行サーバ 103 から電子バリューを受信するためのセッション番号が含まれている。

次に、ユーザが“Receive e-Value”を選択すると、モバイルユーザ端末 101（ブラウザ 401）は、<Go HREF=“wallet:///evReceive”>を実行し、モバイルユーザ端末 101（電子財布 400）は、電子バリュー発行サーバ 103 にアクセスし、スマートカード 307 に格納されているユーザ秘密鍵とユーザ証明書とサービス提

供者証明書を用いて、電子バリュー発行サーバ 103 との間で相互認証を行い暗号化通信セッションを確立し、電子バリューを受信するためのセッション番号をパラメータとして電子バリュー発行サーバ 103 に電子バリューの発行を要求する(2405)。

モバイルユーザ端末 101 から発行要求(2405)を受信した電子バリュー発行サーバ 103 は、モバイルユーザ端末 101 の機種や画面サイズなどの属性を示す端末プロフィールを要求するメッセージ、端末プロフィール要求(2406)をモバイルユーザ端末 101 に送信し、端末プロフィール要求(2406)を受信したモバイルユーザ端末 101 は、端末プロフィール(2407)を電子バリュー発行サーバ 103 に送信する。

図 30 (b) は、モバイルユーザ端末 101 から電子バリュー発行サーバ 103 に送信される端末プロフィール(2407)の一例を示しており、この場合、機種(TerminalType)が、"MT0001"、ブラウザアプリケーションの種類(BrowserType)が"B000B20A"、電子財布アプリケーションの種類(eWalletType)が"W000A10B"、画面(Screen)が、160画素×200画素の8ビットカラー(160x200x8)のモバイルユーザ端末 101であることを示している。

端末プロフィール(2407)を受信した電子バリュー発行サーバ 103 では、電子バリューマネージャ 2201 が、受信した端末プロフィール(2407)をもとに、モバイルユーザ端末 101 の種類に対応した電子バリューを生成する。図 31 は、電子バリューの生成フローを示している。

図 31 において、まず、電子バリューマネージャ 2201 は、電子バリューテンプレートデータベース 2202 をアクセスし、電子バリュー発行要求(2402)の中の電子バリュータイプ(evType)と電子バリューコード(evCode)が示す電子バリューテンプレートデータ 2200 を選択する(電子バリューテンプレート選択 2601)。

次に、電子バリューマネージャ 2201 は、ユーザデータベース 2204 をアクセスして、モバイルユーザ端末 101 の所有者のユーザ情報を取得し、さらに、電子バリューのID(evID)と電子バリュー固有の電子バリュー秘密鍵(evPrivateKey)とその証明書である電子バリュー証明書(evCertificate)を生成して、選択した電子バリューテンプレートデータ 2200 の電子バリューテンプレート 2301 とから、電子バリューのセキュリティ情報部 804 を生成する(セキュリティ情報部生成 2

602)。

次に、電子バリューマネージャ 2201 は、電子バリュー発行要求(2402)に基づいて、電子バリューテンプレート 2301 から電子バリューのプレゼンテーションカード 801 と可変属性 802 を生成する(バリュー属性情報生成 2603)。この時、プレゼンテーションカード 801 にはサービス提供者の署名が施され、可変属性 802 には、電子バリュー秘密鍵(evPrivateKey)による書名が施される。

次に、電子バリューマネージャ 2201 は、電子バリュー発行要求(2402)に基づいて、電子バリューテンプレート 2301 から電子バリューのサービス制御部を生成する(サービス制御部生成 2604)。

次に、電子バリューマネージャ 2201 は、表示制御部生成ルール 2303 のスクリプトプログラムを実行し、受信した端末プロファイル(2407)に適した表示制御情報を表示制御リスト 2302 から選択し、選択した表示制御情報に電子バリューの ID (evID) を付加し、さらに、サービス提供者の署名を施して、電子バリューの表示制御部 1201 を生成する(表示制御部生成 2605)。

次に、電子バリューマネージャ 2201 は、表示リソース部生成ルール 2305 のスクリプトプログラムを実行し、受信した端末プロファイル(2407)に適したイメージデータや音声データを表示リソースリスト 2304 から選択し、選択したイメージデータや音声データを表示リソース部の記述形式に変換して、電子バリューの表示リソース部 1202 を生成して(表示リソース部生成 2606)、電子バリューの生成を完了する。なお、表示リソースリスト 2304 に、端末プロファイル(2407)に適したイメージデータや音声データが無かった場合、電子バリューマネージャ 2201 が、表示リソースリスト 2304 上のデータから端末プロファイル(2407)に適したイメージデータや音声データを生成するようにしてもよい。

電子バリュー発行サーバ 103 の電子バリューマネージャ 2201 は、生成した電子バリューを電子バリューデータベース 2203 に登録し、さらに、電子バリューをモバイルユーザ端末 101 に送信する(2408)。図 3 2 は、図 1 7 に示した電子バリューに対応する電子バリューデータベース 2203 に登録されている電子バリューのマークアップ記述言語に基づくデータ構造を示している。図 1 7 に示したモバイルユーザ端末 101 のスマートカード 307 に格納された状態のものは、マ

ークアップ記述言語による記述の最初の"<Description about="http://www.evaluate.com/evaluate/10000000000000000000000000000001">"の部分だけが異なっている。これは、図 3 2 に示した電子バリューが、"http://www.evaluate.com/evaluate/10000000000000000000000000000001"という識別子で電子バリューデータベース 2203 に管理されていることを示している。

電子バリューを受信したモバイルユーザ端末 101 は、電子バリューデータを生成し、スマートカード 307 に格納して、電子バリューを電子財布 400 に登録する。この時、電子バリューは、図 1 7 に示すように、その最初の部分が"<Description about="wallet:///Evaluate/ev00000033">"と変更される。

以上のように、電子バリュー発行サーバ 103 とモバイルユーザ端末 101 と電子バリューのデータ構造を構成することにより、モバイルユーザ端末 101 の種類に応じた電子バリューを発行することができる。

また、電子バリューが格納されたスマートカード 307 を、画面サイズ等が異なる別機種 of モバイルユーザ端末に装着して、電子バリューを使用する場合や、電子バリューが格納されたスマートカード 307 を、ユーザ端末 107 のスマートカードリーダー 701 に挿入し、ユーザ端末 107 で電子バリューを使用する場合、その端末に対応した表示制御部の実体 1201 と表示リソース部の実体 1202 がダウンロードされ、その端末に適した形式で、電子バリューが表示される。図 2 9 (b) は、この場合 of 電子バリュー of 表示制御部の実体 1201 と表示リソース部の実体 1202 of ダウンロード of 手順を示している。

まず、モバイルユーザ端末 101 (またはユーザ端末 107) は、電子バリュー of 表示制御部 805 で規定されている表示制御部の実体 of URI (図 1 7 に示した電子バリュー of 場合："http://www.evaluate.com/evaluate/ev_0000300000000201/RpCtrl") に基づいて、表示制御部の実体を要求する (表示制御部要求 2411)。表示制御部要求 2411 に対し、電子バリュー発行サーバ 103 (URL ="http://www.evaluate.com") は、モバイルユーザ端末 101 (またはユーザ端末 107) of 機種や画面サイズなどの属性を示す端末プロフィールを要求するメッセージ、端末プロフィール要求 2412 をモバイルユーザ端末 101 に送信し、端末プロフィール要求 2406 を受信したモバイルユーザ端末 101 (またはユーザ端末 107) は、端末プロ

ファイル(2413)を電子バリュー発行サーバ103に送信する。端末プロフィール2413を受信した電子バリュー発行サーバ103は、電子バリューを生成する場合の表示制御部生成2605と同様の手順で、モバイルユーザ端末101（またはユーザ端末107）に適した表示制御部を生成し、生成した表示制御部(2414)をモバイルユーザ端末101（またはユーザ端末107）に送信する。

次に、モバイルユーザ端末101（またはユーザ端末107）は、電子バリューの表示リソース部806で規定されている表示リソース部の実体のURI（図17に示した電子バリューの場合：“http://www.evalue.com/evalue/ev_0000300000000201/RpRes”）に基づいて、表示リソース部の実体を要求する（表示リソース部要求2415）。表示リソース部要求2415に対し、電子バリュー発行サーバ103（URL=“<http://www.evalue.com>”）は、電子バリューを生成する場合の表示リソース部生成2606と同様の手順で、モバイルユーザ端末101（またはユーザ端末107）に適した表示リソース部を生成し、生成した表示リソース部(2416)をモバイルユーザ端末101（またはユーザ端末107）に送信する。

モバイルユーザ端末101（またはユーザ端末107）は、電子バリュー発行サーバ103からダウンロードした表示制御部（実体）と表示リソース部（実体）とスマートカード307に格納されていた電子バリューデータとから電子バリューオブジェクトを生成して、電子バリューを最適な形式で画面に表示する。

この時、モバイルユーザ端末101（またはユーザ端末107）の種類に応じて変更されるのは、電子バリューの表示に関する部分のみであり、この機能を悪用して、電子バリューのプレゼンテーションカード801や、可変情報802、サービス制御部803、セキュリティ情報部804を不正に改ざんすることはできない。

以上のように、電子バリュー発行サーバ103とモバイルユーザ端末101とユーザ端末107及び電子バリューのデータ構造を構成することにより、電子バリューの改ざん等の不正行為に対するセキュリティを確保しつつ、電子バリューを表示する端末（モバイルユーザ端末101またはユーザ端末107）の端末プロフィールに応じて、多彩な表現力を持った電子バリューを扱うことができる。これにより、単にカラフルな電子バリューが扱えるだけでなく、電子バリューを広告メディアとしても利用することが可能となる。この場合、サービス提供者の広告収入の一

部をユーザに還元し、電子バリューをユーザに割引いて販売したり、懸賞の商品として電子バリューをユーザに無料で配布するといった利用の仕方も可能となり、しいては、モバイル・エレクトロニックコマース・サービスの利用を促進させることができる。

なお、以上に述べた構成では、モバイルユーザ端末 101 とサービス端末 105 との通信に赤外線通信を用いたが、その他の無線通信方式を用いてもよく、その場合、モバイルユーザ端末 101 は赤外線通信モジュール 111 の代わりにその無線通信方式の無線通信手段を、サービス端末 105 は、赤外線通信アダプタ 602 の代わりにその無線通信方式の無線通信手段をそれぞれ備える。

また、以上の説明では、モバイル・エレクトロニックコマース・システムを構成するモバイルユーザ端末 101 は、モバイル・エレクトロニックコマース・サービスにおける機能を実現するための、最適なハードウェア構成を備えているが、機能としては、デジタル無線通信機能と、赤外線通信機能、及び、スマートカードリーダーライタと、ディスプレイと、キーボード（または、ペン入力デバイス）と、マイクと、スピーカとを備えたコンピュータによって構成することもできる。この場合、FeRAM301 に格納されているプログラムを、パソコンのOS (Operating System) 上で動作するソフトウェア・プログラムに変換し、そのソフトウェア・プログラムを、コンピュータから実行可能な場所（例：ハードディスク）に格納しておく。

実施例 2

本発明の形態は、第 1 の実施例におけるモバイル・エレクトロニックコマース・システムを、モバイルユーザ端末とサービス端末との改札決済処理において、ユーザの操作性を損なうことなく、より安定的な決済処理ができるように、モバイルユーザ端末 101 とサービス端末 105 を構成したものである。

本実施例におけるモバイルユーザ端末 101 は、図 3 3 (a)、(b) 及び図 3 4 に示すように、赤外線通信ポート 211 (赤外線通信モジュール) とブルー투스モジュール 2800 を備えている。一方、サービス端末 105 は、図 3 5 に示すように、赤外線通信アダプタ 602 とブルー투스アダプタ 3000 を備えている。モバイルユーザ端末 101 とサービス端末 105 は、赤外線通信とブルーツースの 2 種

類の無線通信手段を用いて改札決済処理を行う。

ユーザの操作は、第1及び第2の実施例の場合と同様に、モバイルユーザ端末101の赤外線通信ポート211（赤外線通信モジュール）を、改札決済処理を行うサービス端末105の赤外線通信アダプタ602に向けて、改札決済処理の開始操作（改札決済処理の実行に割り付けられたファンクションスイッチを押す）を行うだけで良い。この時、モバイルユーザ端末101とサービス端末105は、以下に示す手順を基本の手順として、札決済処理を行う。

まず、モバイルユーザ端末101と赤外線通信ポート211が向けられたサービス端末105との間で、ブルーツースで通信を開始するための情報（デバイスアドレス、セッション番号）を赤外線通信によって交換し、次に、赤外線通信によって交換した情報（デバイスアドレス、セッション番号）をもとに、モバイルユーザ端末101とサービス端末105との間で、ブルーツースによる通信セッションを確立し、さらに、第1の実施例で示した5つのメッセージプレゼンテーション1003、インストラクション1004、トランザクション1005、Receipt1006、アクノーリッジ1007をブルーツースで交換し、改札決済処理を完了する。

このように、ブルーツースで通信する前段階として、指向性が高い赤外線通信を用いて、ブルーツースで通信を開始するための情報（デバイスアドレス、セッション番号）を交換することにより、不特定な相手同士であっても、赤外線通信ポートを相手に向けるという直感的で簡単な操作で、選択的に相手とブルーツースで通信することが出来る。ブルーツースによる通信セッションを確立するまでの手順に関しては、複数パターンの実施例が可能であり、ここでは、2つのパターンの処理手順について説明する。

（パターン1）

図36（a）、（b）は、それぞれ、パターン1の場合のモバイルユーザ端末101とサービス端末105の改札決済処理の手順を示している。

パターン1の場合、最初に、サービス端末105は、ユーザが改札決済処理の開始操作を行い、モバイルユーザ端末からブルーツースによる認証処理要求を受信するまで（手順3110）、サービス端末105との通信方法を指示するメッセージ、Initiationメッセージを、赤外線通信によって連続的に送信している（手順3109）。

この場合、Initiation メッセージには、サービス端末 105 のブルーツースのデバイスアドレスと、サービス端末が任意に設定したブルーツースによる通信セッションを識別するセッション番号が含まれている。

一方、モバイルユーザ端末 101 は、ユーザが改札決済処理の開始操作を行うと、赤外線通信ポート 211（赤外線通信モジュール）を介して、サービス端末 105 から Initiation メッセージを受信し（手順 3101）、次に、Initiation メッセージに含まれるサービス端末のブルーツースのデバイスアドレスをもとに、ブルーツースのデバイスリストからサービス端末 105 を検索し（手順 3102）で、サービス端末 105 にブルーツースによる認証処理を要求する（手順 3103）。

この後、モバイルユーザ端末 101 とサービス端末 105 とは、それぞれ、手順 3104 と手順 3111 とにおいて、ブルーツースの認証処理の手順に基づいて相互認証を行い、手順 3105 と手順 3112 とにおいて、ブルーツースの通信セッションを確立する。

次に、モバイルユーザ端末 101 とサービス端末 105 とは、それぞれ、手順 3106 と手順 3113 とにおいて、セッション番号照合処理を行う。具体的には、モバイルユーザ端末 101 は、Initiation メッセージに含まれていたセッション番号を、サービス端末 105 にブルーツースによって送信し、一方、サービス端末 105 は、受信したセッション番号を、Initiation メッセージの一部として送信したセッション番号と照合して、ブルーツースによる通信セッションを識別する。

次に、モバイルユーザ端末 101 とサービス端末 105 とは、それぞれ、手順 3107 と手順 3114 とにおいて、ブルーツースによってプレゼンテーション 1003、インスタクション 1004、トランザクション 1005、Receipt 1006、アクノーリッジ 1007 の 5 つのメッセージを交換し、それぞれ、手順 3108 と手順 3115 とにおいて、ブルーツースの通信セッションを切断し、決済改札処理を完了する。

また、モバイルユーザ端末 101 は、手順 3102 において、ブルーツースのデバイスリストに該当するサービス端末 105 がなかった場合、または、手順 3104 のブルーツースの認証処理においてエラーが発生した場合、または、手順 3106 のセッション番号照合処理においてエラーが発生した場合、または、手順 3107 の 5 つのメッセージの交換においてエラーが発生した場合、ディスプレイ a21-00 に、

そのエラーの内容を示すエラーメッセージを表示し、改札決済処理を中止する。

また、サービス端末 105 は、手順 3111 のブルーツースの認証処理においてエラーが発生した場合、または、手順 3113 のセッション番号照合処理においてエラーが発生した場合、または、手順 3114 の 5 つのメッセージの交換においてエラーが発生した場合、改札決済処理を中止する。

なお、以上では、モバイルユーザ端末 101 は、手順 3101 において、サービス端末 105 から Initiation メッセージを赤外線通信によって受信したが、その直後に、モバイルユーザ端末 101 からサービス端末 105 に Initiation メッセージを赤外線通信によって送信して、お互いの Initiation メッセージを交換するようにしても良い。この場合、モバイルユーザ端末 101 からサービス端末 105 に送信される Initiation メッセージには、モバイルユーザ端末 101 のブルーツースのデバイスアドレスと、モバイルユーザ端末 101 が任意に設定したブルーツースによる通信セッションを識別するセッション番号が含まれている。モバイルユーザ端末 101 とサービス端末 105 とは、それぞれ、手順 3106 と手順 3113 とにおいて、それぞれが任意に設定したセッション番号を照合して、赤外線通信によって Initiation メッセージを交換した相手同士であることを相互に認証することができ、通信のセキュリティを高めることが出来る。

また、以上では、必ず、赤外線通信とブルーツースの両方を用いる場合について説明したが、Initiation メッセージの中に、5 つのメッセージを交換する際の通信手段を指定する情報を含めるようにしても良い。例えば、赤外線通信が指定された場合には、モバイルユーザ端末 101 とサービス端末 105 とはブルーツースによる通信は行わず、赤外線通信によって 5 つのメッセージを交換し、改札決済処理を完了する。

(パターン 2)

図 37 (a)、(b) は、それぞれ、パターン 2 の場合のモバイルユーザ端末 101 とサービス端末 105 の改札決済処理の手順を示している。

パターン 2 の場合、最初に、モバイルユーザ端末 101 は、ユーザが改札決済処理の開始操作を行うと、サービス端末からブルーツースによる認証処理要求を受信するまで(手順 3202)、モバイルユーザ端末 101 との通信方法を指示するメッ

セージ、Initiation メッセージを、赤外線通信によって連続的に送信している（手順 3201）。この場合、Initiation メッセージには、モバイルユーザ端末 101 のブルーツースのデバイスアドレスと、モバイルユーザ端末が任意に設定したブルーツースによる通信セッションを識別するセッション番号が含まれている。

一方、サービス端末 105 は、ユーザが改札決済処理の開始操作を行うと、赤外線通信ポート 211（赤外線通信モジュール）を介して、モバイルユーザ端末 101 から Initiation メッセージを受信し（手順 3208）、次に、Initiation メッセージに含まれるモバイルユーザ端末のブルーツースのデバイスアドレスをもとに、ブルーツースのデバイスリストからモバイルユーザ端末 101 を検索し（手順 3209）て、モバイルユーザ端末 101 にブルーツースによる認証処理を要求する（手順 3210）。

この後、モバイルユーザ端末 101 とサービス端末 105 とは、それぞれ、手順 3203 と手順 3211 とにおいて、ブルーツースの認証処理の手順に基づいて相互認証を行い、手順 3204 と手順 3212 とにおいて、ブルーツースの通信セッションを確立する。

次に、モバイルユーザ端末 101 とサービス端末 105 とは、それぞれ、手順 3205 と手順 3213 とにおいて、セッション番号照合処理を行う。具体的には、サービス端末 105 は、Initiation メッセージに含まれていたセッション番号を、モバイルユーザ端末 101 にブルーツースによって送信し、一方、モバイルユーザ端末 101 は、受信したセッション番号を、Initiation メッセージの一部として送信したセッション番号と照合して、ブルーツースによる通信セッションを識別する。

次に、モバイルユーザ端末 101 とサービス端末 105 とは、それぞれ、手順 3206 と手順 3214 とにおいて、ブルーツースによってプレゼンテーション 1003、インスタクション 1004、トランザクション 1005、Receipt 1006、アクノーリッジ 1007 の 5 つのメッセージを交換し、それぞれ、手順 3207 と手順 3215 とにおいて、ブルーツースの通信セッションを切断し、決済改札処理を完了する。

また、モバイルユーザ端末 101 は、手順 3203 のブルーツースの認証処理においてエラーが発生した場合、または、手順 3205 のセッション番号照合処理にお

いてエラーが発生した場合、または、手順 3206 の 5 つのメッセージの交換においてエラーが発生した場合、ディスプレイ 200 に、そのエラーの内容を示すエラーメッセージを表示し、改札決済処理を中止する。

また、サービス端末 105 は、手順 3209 において、ブルーツースのデバイスリストに該当するモバイルユーザ端末 101 がなかった場合、または、手順 3211 のブルーツースの認証処理においてエラーが発生した場合、または、手順 3213 のセッション番号照合処理においてエラーが発生した場合、または、手順 3214 の 5 つのメッセージの交換においてエラーが発生した場合、改札決済処理を中止する。

なお、以上では、モバイルユーザ端末 101 は、手順 3201 において、モバイルユーザ端末 101 から Initiation メッセージを赤外線通信によって受信したが、その直後に、サービス端末 105 からモバイルユーザ端末 101 に Initiation メッセージを赤外線通信によって送信して、お互いの Initiation メッセージを交換するようにしても良い。この場合、サービス端末 105 からモバイルユーザ端末 101 に送信される Initiation メッセージには、サービス端末 105 のブルーツースのデバイスアドレスと、サービス端末 105 が任意に設定したブルーツースによる通信セッションを識別するセッション番号が含まれている。モバイルユーザ端末 101 とサービス端末 105 とは、それぞれ、手順 3205 と手順 3213 とにおいて、それぞれが任意に設定したセッション番号を照合して、赤外線通信によって Initiation メッセージを交換した相手同士であることを相互に認証することができ、通信のセキュリティを高めることが出来る。

また、以上では、必ず、赤外線通信とブルーツースの両方を用いる場合について説明したが、Initiation メッセージの中に、5 つのメッセージを交換する際の通信手段を指定する情報を含めるようにしても良い。例えば、赤外線通信が指定された場合には、モバイルユーザ端末 101 とサービス端末 105 とはブルーツースによる通信は行わず、赤外線通信によって 5 つのメッセージを交換し、改札決済処理を完了する。

【発明の効果】

以上のように、本発明によれば、固有の秘密鍵とその証明書と、その秘密鍵に

よって署名された情報とを備えた電子情報を、保存管理する手段を電子財布に備えたものである。これにより、電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

また、本発明では、電子財布に格納される電子情報と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された、固定属性情報と表示制御情報をさらに備え、これら3つの情報を用いて表示データを生成するようにすることもできる。これにより、電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

また、本発明では、電子財布に格納される電子情報と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報を有するとともに、表示制御情報を取得するための情報をさらに備えることもできる。電子情報の発行者が規定する情報を、電子情報に入れることが出来る。

また、本発明では、電子財布に格納される電子情報と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報を有するとともに、電子情報の発行者によって署名され或いは署名されていない表示リソース取得するための情報をさらに備え、これら3つの情報を用いて表示データを生成するようにすることもできる。これにより、電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。また、電子情報の発行者が規定する情報を、電子情報に入れることが出来る。

また、本発明では、電子財布に格納される電子情報と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報とを有するとともに、表示制御情報の識別情報及び電子情報の発行者によって署名され或いは署名されていない表示リソースを取得するための情報をさらに備えることもできる。これにより、電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。また、電子情報の発行者が規定する情報を、電子情報に入れることが出来る。

また、本発明では、電子財布に格納される電子情報と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名され

た固定属性情報とを有するとともに、電子情報ハンドラの認証鍵をさらに備え、前記電子情報ハンドラに、電子情報を有する端末との間で決済処理を行なわせるようにすることにより、電子情報ハンドラの認証鍵によって、電子情報ハンドラを認証することができ、安全性が向上する。

また、本発明では、電子財布に格納される電子情報と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報とを有するとともに、表示制御情報を取得するための情報と、表示リソースを取得するための情報及び電子情報ハンドラの認証鍵を備えることもできる。電子情報ハンドラの認証鍵によって、電子情報ハンドラを認証することができ、安全性が向上する。

また、本発明では、電子財布に格納される電子情報と同様、秘密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報とを有するとともに、サービス制御情報をさらに備え、前記サービス制御情報は、電子情報により行なう決済処理を規定するようにすることもできる。これにより、サービス制御情報を変更することにより、各種の電子情報を規定することができる。

また、本発明では、電子財布に格納される電子情報と同様、密鍵によって署名された情報が可変属性情報であり、また、電子情報の発行者によって署名された固定属性情報とを有するとともに、表示制御情報を取得するための情報と、表示リソースを取得するための情報と、電子情報ハンドラの認証鍵及びサービス制御情報をさらに備えることもできる。

これにより、サービス制御情報を変更することにより、各種の電子情報を規定することができる。

また、本発明では、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備え、前記電子情報オブジェクトが、決済処理を実行する際に、交換する各メッセージに、前記サービス制御情報に基づく決済処理データを埋め込むようにすることが可能である。これにより、電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

また、本発明では、前記サービス制御情報が、サービス制御モジュール情報の

組合せから成るようにすることができる。サービス制御モジュール情報の組み合わせを変更することにより各種の電子情報を規定することができる。

また、本発明では、前記電子情報オブジェクトが、決済処理を実行する際に、決済処理に交換する各メッセージに埋め込まれるサービス制御情報に基づく決済処理メッセージが、電子情報から電子情報ハンドラに決済処理を申し出るメッセージであるようにすることができる。各種の電子情報における決済処理を、効率的に行うことが出来る。

また、本発明では、前記電子情報オブジェクトが、決済処理を実行する際に、決済処理に交換する各メッセージに埋め込まれるサービス制御情報に基づく決済処理メッセージが、電子情報ハンドラから電子情報に属性値の変更を命令するメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

また、本発明では、前記電子情報オブジェクトが、決済処理を実行する際に、決済処理に交換する各メッセージに埋め込まれるサービス制御情報に基づく決済処理メッセージが、電子情報から電子情報ハンドラに属性値の変更結果を示すメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

また、本発明では、前記電子情報オブジェクトが、決済処理を実行する際に、決済処理に交換する各メッセージに埋め込まれるサービス制御情報に基づく決済処理メッセージが、電子情報ハンドラから電子情報への領収書に相当するメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

請 求 の 範 囲

1 固有の秘密鍵と、その証明書組と、前記秘密鍵によって署名された情報とを備えた電子情報を保存管理する手段を備えた電子財布。

2 秘密鍵によって署名された情報が可変情報であることを特徴とする請求項1記載の電子財布。

3 電子情報の発行者によって署名された情報をさらに備えたことを特徴とする請求項1記載の電子財布。

4 秘密鍵によって署名された情報が可変情報であり、また、電子情報の発行者によって署名された固定情報をさらに備えたことを特徴とする請求項1記載の電子財布。

5 秘密鍵によって署名された情報が可変情報であり、また、電子情報の発行者によって署名された固定情報と表示制御情報をさらに備え、これら3つの情報を用いて表示データを生成することを特徴とする請求項1記載の電子財布。

6 秘密鍵によって署名された情報が可変情報であり、また、電子情報の発行者によって署名された固定情報と表示制御情報を取得するための情報とをさらに備えたことを特徴とする請求項1記載の電子財布。

7 秘密鍵によって署名された情報が可変情報であり、また、電子情報の発行者によって署名された固定情報と、電子情報の発行者によって署名され或いは署名されていない表示リソースをさらに備え、これら3つの情報を用いて表示データを生成することを特徴とする請求項1記載の電子財布。

8 秘密鍵によって署名された情報が可変情報であり、また、電子情報の発行者によって署名された固定情報と、電子情報の発行者によって署名され或いは署名されていない表示リソースを取得するための情報をさらに備えたことを特徴とする請求項1記載の電子財布。

9 秘密鍵によって署名された情報が可変情報であり、また、電子情報の発行者によって署名された、固定情報及び電子ハンドラの認証鍵をさらに備え、前記電子情報ハンドラは、電子情報を有する端末との間で決済処理を行なうことを特徴とする請求項1記載の電子財布。

1 0 秘密鍵によって署名された情報が可変情報であり、また、電子情報の発行者によって署名された、固定情報とサービス制御情報をさらに備え、サービス制御情報は、電子情報により行なう決済処理を規定することを特徴とする請求項 1 記載の電子財布。

1 1 電子情報から電子情報オブジェクトを生成する手段を備え、前記電子情報オブジェクトは、秘密鍵とその証明書を内部変数として有することを特徴とする請求項 1 乃至 1 0 のいずれかに記載の電子財布。

1 2 電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備え、また、前記電子情報オブジェクトが、決済処理時に交換する各メッセージに、前記サービス制御情報に基づく決済処理データを埋め込むことを特徴とする請求項 1 0 記載の電子財布。

1 3 サービス制御情報は、サービス制御モジュール情報の組合せから成ることを特徴とする請求項 1 2 記載の電子財布。

1 4 電子情報オブジェクトによりサービス制御情報に埋め込まれるメッセージが、電子情報オブジェクトから電子情報ハンドラに決済処理を申し出るメッセージであることを特徴とする請求項 1 2 記載の電子財布。

1 5 電子情報オブジェクトによりサービス制御情報に埋め込まれるメッセージが、電子情報ハンドラから電子情報オブジェクトに属性値の変更を命令するメッセージであることを特徴とする請求項 1 2 記載の電子財布。

1 6 電子情報オブジェクトによりサービス制御情報に埋め込まれるメッセージが、電子情報オブジェクトから電子情報ハンドラに属性値の変更結果を示すメッセージであることを特徴とする請求項 1 2 記載の電子財布。

1 7 電子情報オブジェクトによりサービス制御情報に埋め込まれるメッセージが、電子情報ハンドラから電子情報への領収書に相当するメッセージであることを特徴とする請求項 1 2 記載の電子財布。

1 8 電子情報ハンドラの発行者によって署名された、固定情報と電子情報オブジェクトの認証鍵とを備えた電子情報ハンドラを保存管理する手段を備えたサービス端末。

19 電子情報ハンドラの発行者によって署名された、固定情報とサービス制御情報と電子情報オブジェクトの認証鍵とを備えた電子情報ハンドラを保存管理する手段を備えたサービス端末。

20 前記電子情報ハンドラを構成する前記サービス制御情報が、サービス制御モジュール情報の組合せであることを特徴とする請求項19記載のサービス端末。

21 前記電子情報ハンドラから電子情報ハンドラオブジェクトを生成し前記電子情報ハンドラを制御する手段を備えた請求項20記載のサービス端末。

22 前記電子情報ハンドラの電子情報ハンドラオブジェクトが、決済処理時に交換する各メッセージに、前記サービス制御情報に基づく決済処理データを埋め込むことを特徴とする請求項19記載のサービス端末。

23 前記電子情報ハンドラの電子情報ハンドラオブジェクトが、決済処理時に交換する各メッセージに、前記サービス制御モジュール情報の組合せに基づく決済処理データを埋め込むことを特徴とする請求項20記載のサービス端末。

24 前記電子情報ハンドラの電子情報ハンドラオブジェクトが決済データを重畳するメッセージが、電子情報から電子情報ハンドラに決済処理を申し出るメッセージと、電子情報ハンドラから電子情報に属性値の変更を命令するメッセージと、電子情報から電子情報ハンドラに属性値の変更結果を示すメッセージと、電子情報ハンドラから電子情報への領収書に相当するメッセージであることを特徴とする請求項23または請求項24記載のサービス端末。

25 電子情報の固有の秘密鍵と可変情報とを生成し、前記可変情報に前記固有の秘密鍵による署名を施すことを特徴とする電子情報生成方法。

26 電子情報の固有の秘密鍵と可変情報と固定情報を生成し、前記可変情報に前記固有の秘密鍵による署名を施し、前記固定情報に電子情報の発行者による署名を施すことを特徴とする電子情報生成方法。

27 電子情報の固有の秘密鍵と可変情報と固定情報と表示制御情報と表示リソースとを生成し、前記可変情報に前記固有の秘密鍵による署名を施し、前記固定情報と前記表示制御情報の識別情報と前記表示リソースの識別情報とに電子情

報の発行者による署名を施すことを特徴とする電子情報生成方法。

28 電子情報の固有の秘密鍵と可変情報と固定情報とサービス制御情報と表示制御情報と表示リソースとを生成し、前記可変情報に前記固有の秘密鍵による署名を施し、前記固定情報と前記サービス制御情報と前記表示制御情報の識別情報と前記表示リソースの識別情報とに電子情報の発行者による署名を施すことを特徴とする電子情報生成方法。

29 電子財布のプロパティに対応して、電子情報の表示制御情報と表示リソースとを生成し、前記表示制御情報に発行者による署名を施すことを特徴とする請求項25から請求項28のいずれかに記載の電子情報生成方法。

30 少なくとも2種類以上の無線通信手段を備え、第1の無線通信手段を用いて相手側の機器からイニシエーションメッセージを取得し、次に第2の無線通信手段において通信が可能な機器の中から、イニシエーションメッセージに含まれる相手側の機器の識別情報が示す機器を選択し、前記相手側の機器と通信セッションを確立し、前記第2の無線通信手段を用いて通信を開始することを特徴とする通信方式。

31 イニシエーションメッセージの中に、相手側の機器の識別情報と共に、相手側の機器が任意に設定した通信セッションの識別情報が含まれ、前記第2の無線通信手段において相手側の機器と通信セッションを確立する際に、前記通信セッションの識別情報を用いて認証処理をすることを特徴とする請求項30記載の通信方式。

32 少なくとも2種類以上の無線通信手段を備え、第1の無線通信手段を用いて、自己の識別情報を含むイニシエーションメッセージを相手側の機器に送信し、次に前記相手側の機器からの第2の無線通信手段による通信セッションの確立要求に対し、前記相手側の機器と通信セッションを確立し、前記第2の無線通信手段を用いて通信を開始することを特徴とする通信方式。

33 イニシエーションメッセージの中に、自己の識別情報と共に、任意に設定した通信セッションの識別情報を含め、前記第2の無線通信手段において前記相手側の機器と通信セッションを確立する際に、前記通信セッションの識別情報

を用いて認証処理をすることを特徴とする請求項 3 2 記載の通信方式。

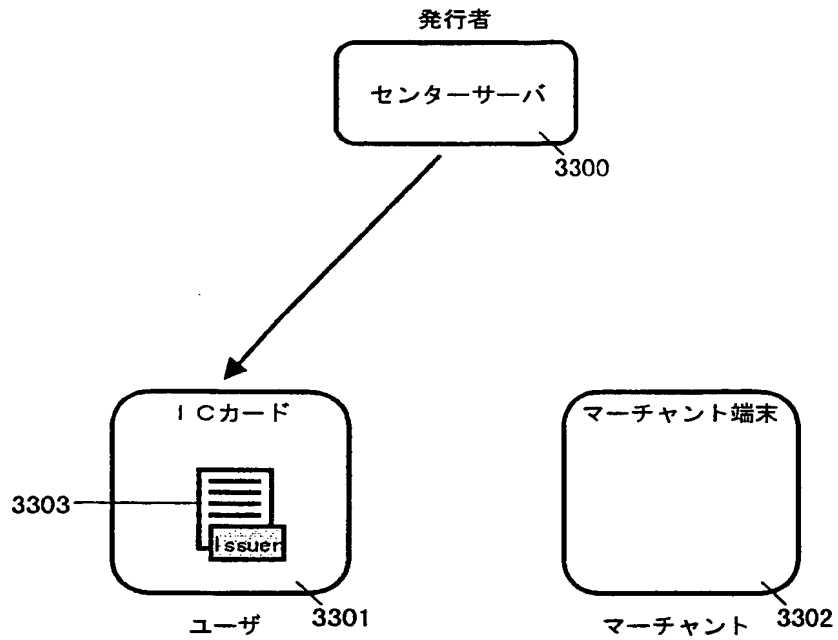
3 4 少なくとも 2 種類以上の無線通信手段を備え、第 1 の無線通信手段を用いて、お互いに自己の識別情報を含むイニシエーションメッセージを交換し、次に前記イニシエーションメッセージを交換した相手側の機器からの第 2 の無線通信手段による通信セッションの確立要求に対し、イニシエーションメッセージに含まれる相手側の機器の識別情報を照合して相手側機器を認証した上で、前記相手側の機器と通信セッションを確立し、前記第 2 の無線通信手段を用いて通信を開始することを特徴とする通信方式。

3 5 イニシエーションメッセージの中に、第 2 の無線通信手段として用いる無線通信手段の識別情報が含まれ、その識別情報が示す無線通信手段を第 2 の無線通信手段として、相手側の機器と通信セッションを確立し、前記第 2 の無線通信手段を用いて通信を開始することを特徴とする請求項 3 0 から請求項 3 4 のいずれかに記載の通信方式。

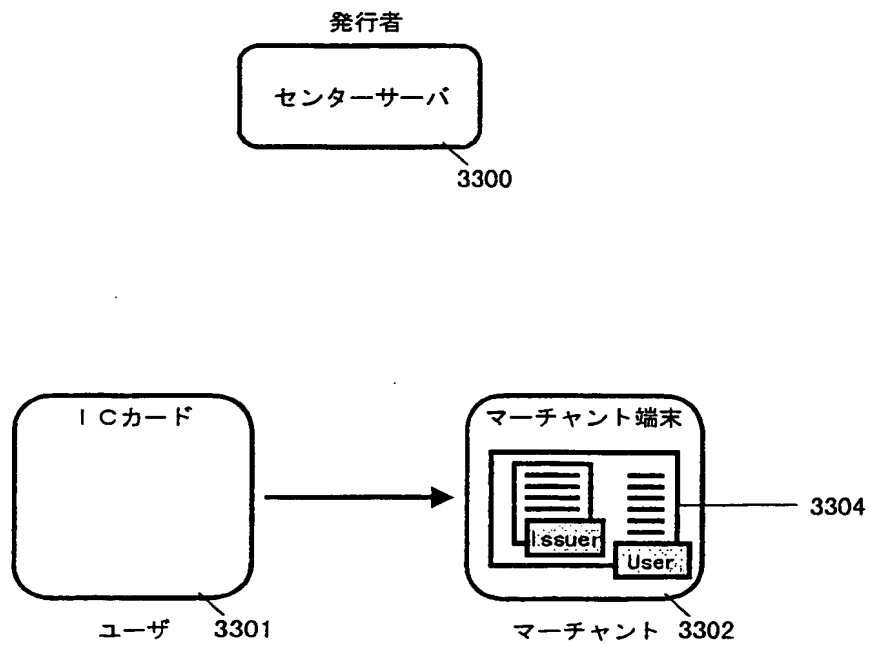
1 / 37

図 1

(a)

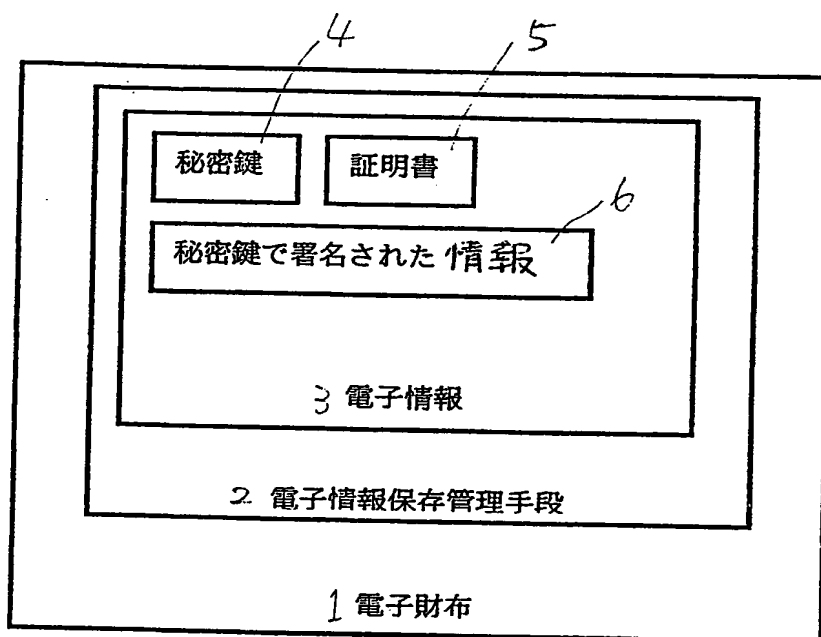


(b)



THIS PAGE BLANK (USPTO)

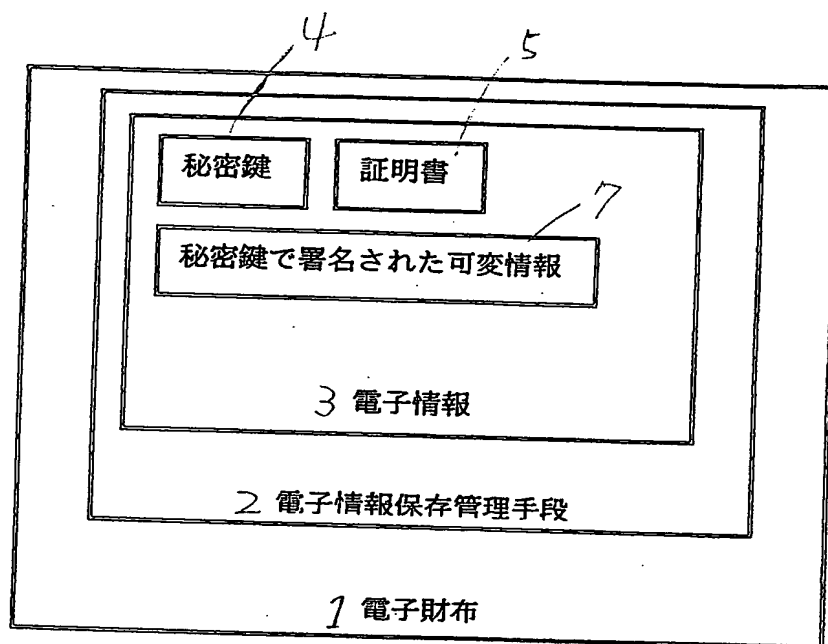
図 2



THIS PAGE BLANK (USPTO)

3 / 37

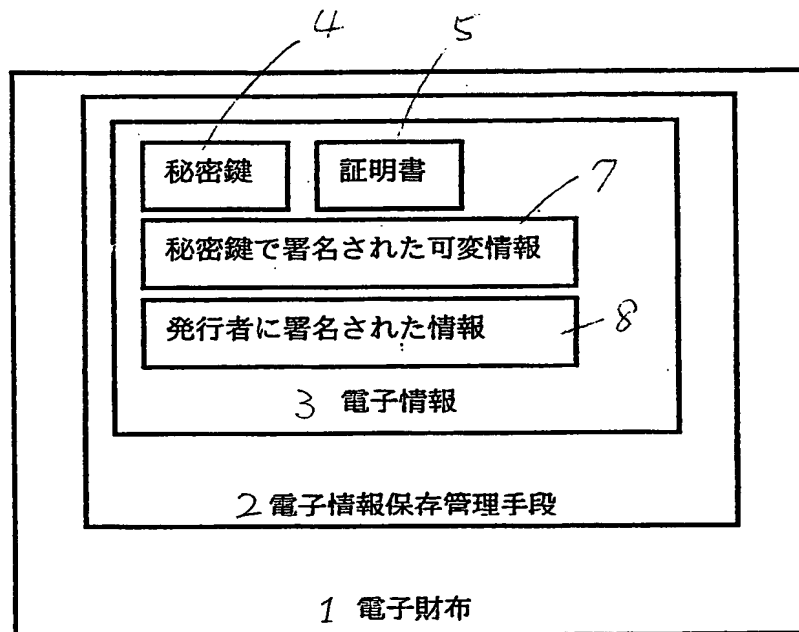
図 3



THIS PAGE BLANK (USPTO)

4 / 3 7

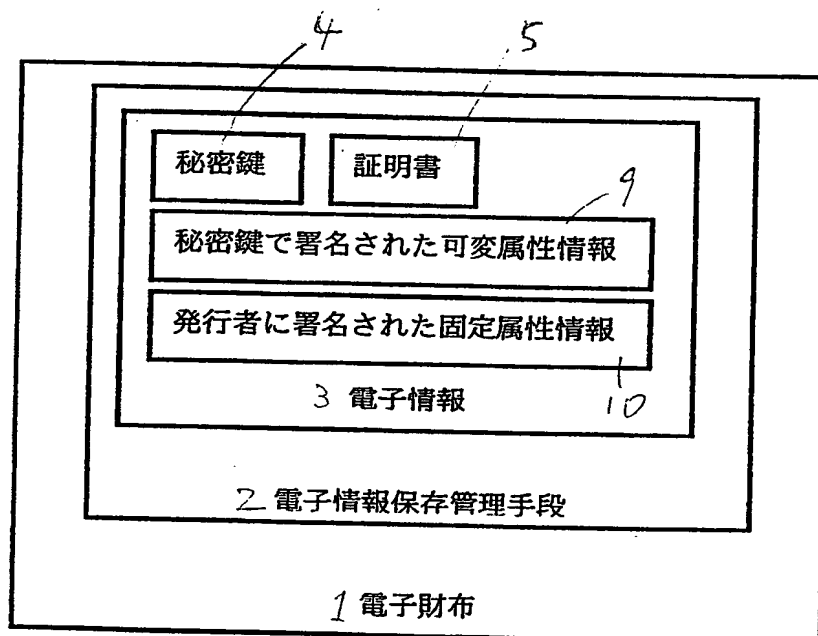
図 4



THIS PAGE BLANK (USPTO)

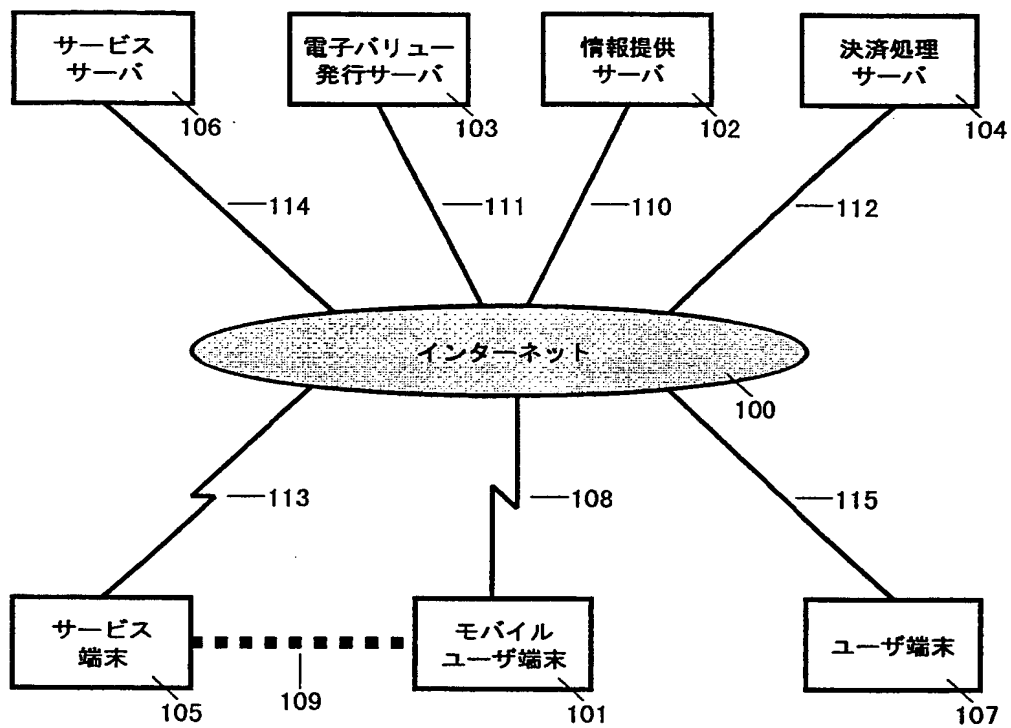
5 / 37

図 5



THIS PAGE BLANK (USPTO)

図 6

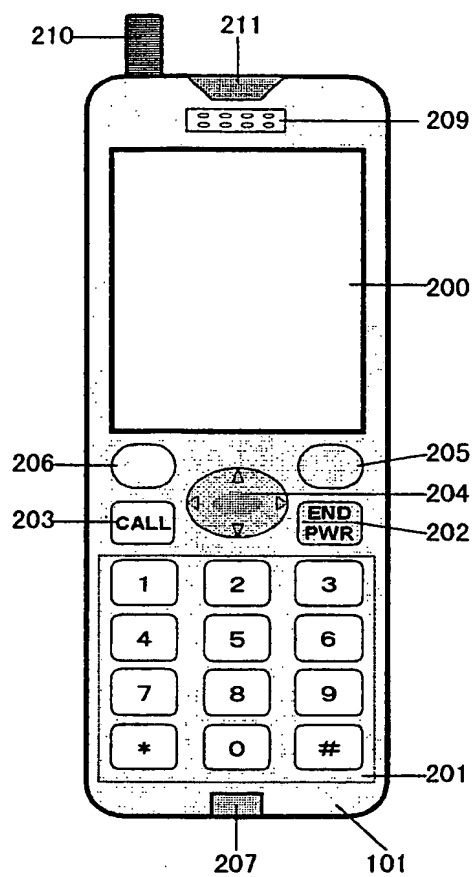


THIS PAGE BLANK (USPTO)

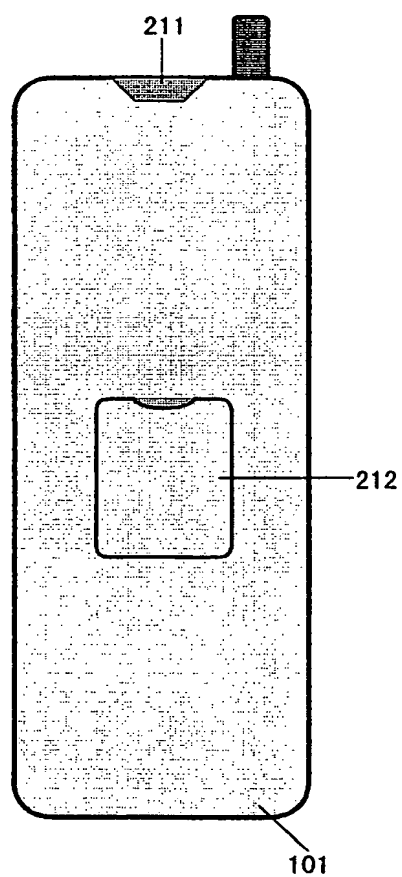
7 / 3 7

図 7

(a)



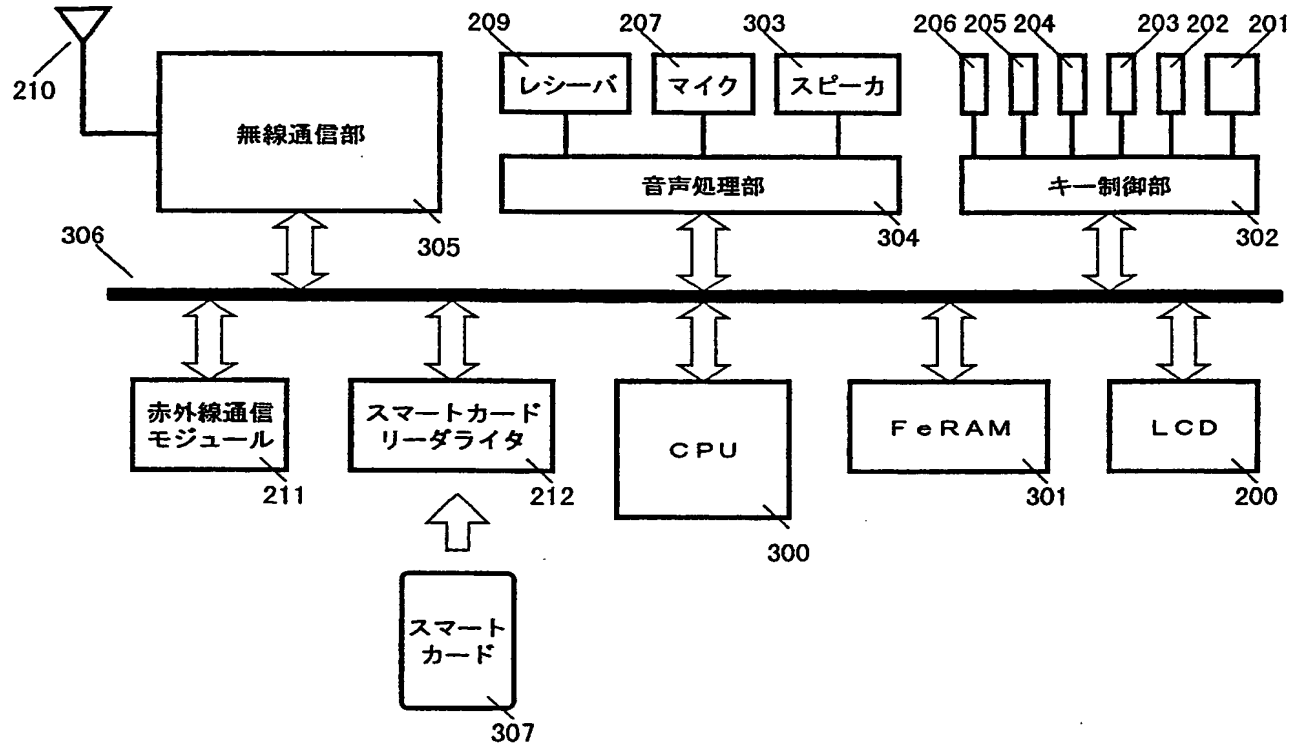
(b)



THIS PAGE BLANK (USPTO)

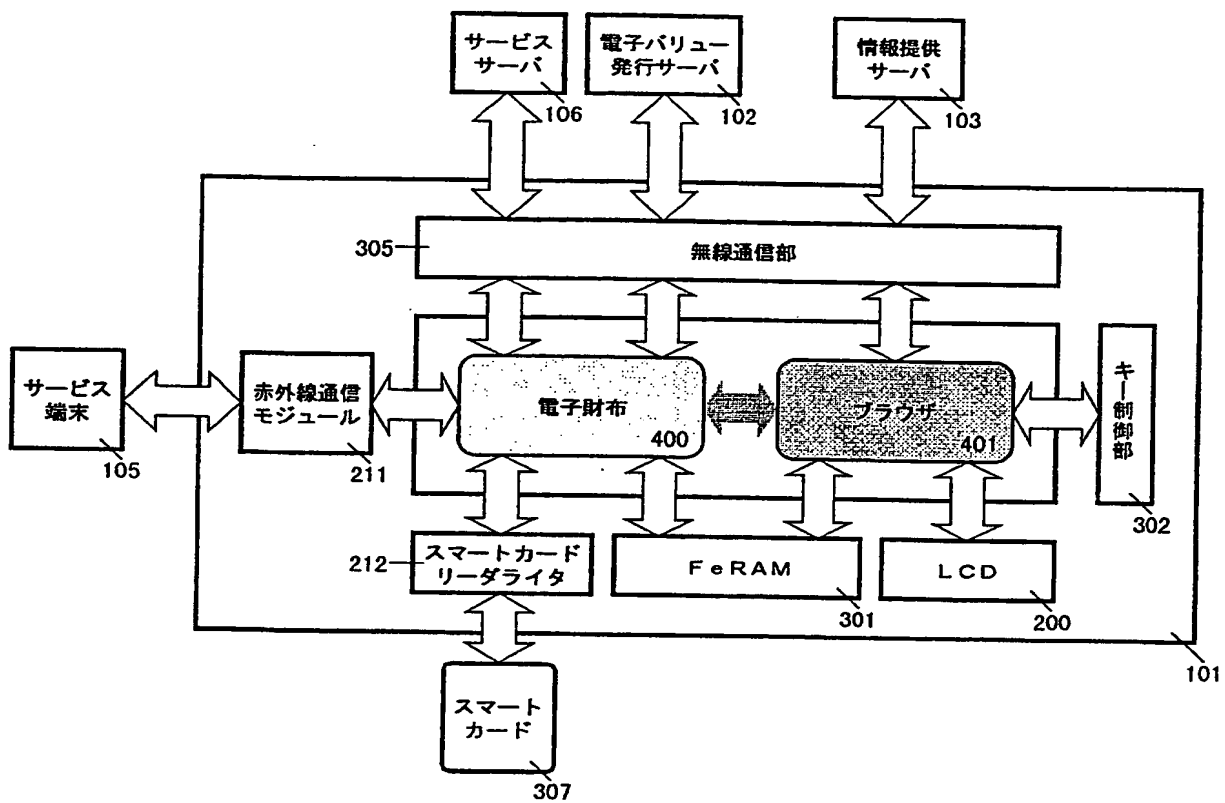
8 / 37

図 8



THIS PAGE BLANK (USPTO)

図 9

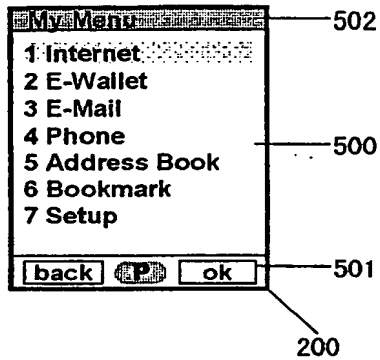


THIS PAGE BLANK (USPTO)

10 / 37


☒ 10

(a)



My Menu

- 1 Internet
- 2 E-Wallet
- 3 E-Mail
- 4 Phone
- 5 Address Book
- 6 Bookmark
- 7 Setup

back  ok

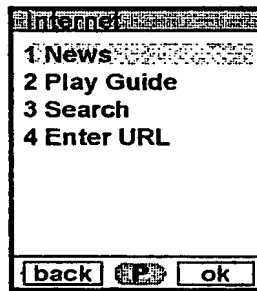
502

500

501


200

(b)

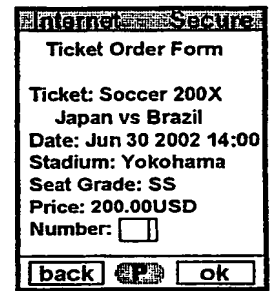


Internet

- 1 News
- 2 Play Guide
- 3 Search
- 4 Enter URL

back  ok


(c)



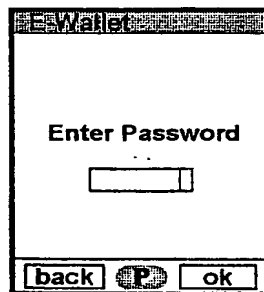
Internet Secure

Ticket Order Form

Ticket: Soccer 200X
Japan vs Brazil
Date: Jun 30 2002 14:00
Stadium: Yokohama
Seat Grade: SS
Price: 200.00USD
Number:


back  ok

(d)

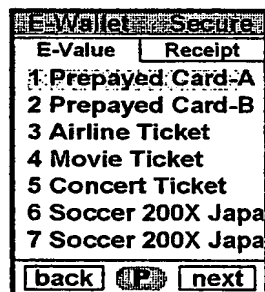


E-Wallet

Enter Password

back  ok


(e)



E-Wallet Secure

E-Value Receipt

- 1 Prepayed Card-A
- 2 Prepayed Card-B
- 3 Airline Ticket
- 4 Movie Ticket
- 5 Concert Ticket
- 6 Soccer 200X Japa
- 7 Soccer 200X Japa

back  next

(f)



E-Wallet Secure

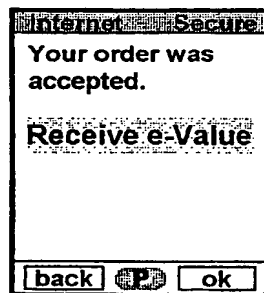
Soccer 200X
Japan vs Brazil



Date: 2002/06/30 14:00
Stadium: Yokohama
Seat: SS-A-28

back  ok


(g)



Internet Secure

Your order was
accepted.

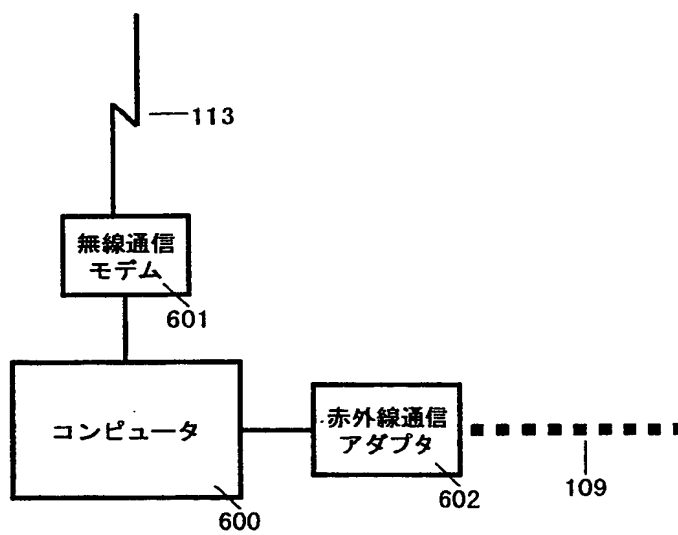
Receive e-Value

back  ok

THIS PAGE BLANK (USPTO)

11 / 37

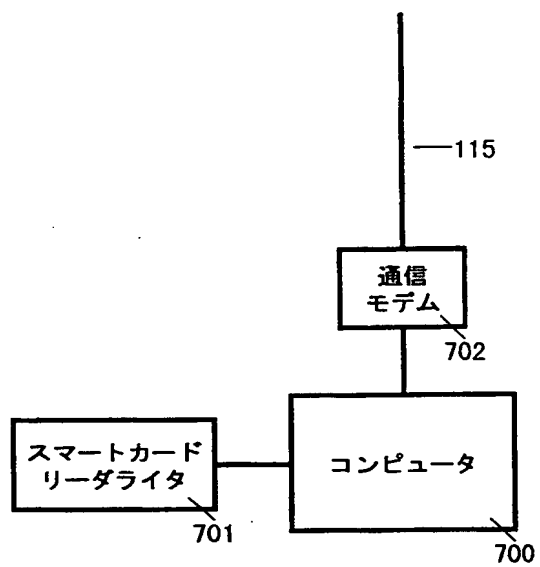
図 11



THIS PAGE BLANK (USPTO)

1 2 / 3 7

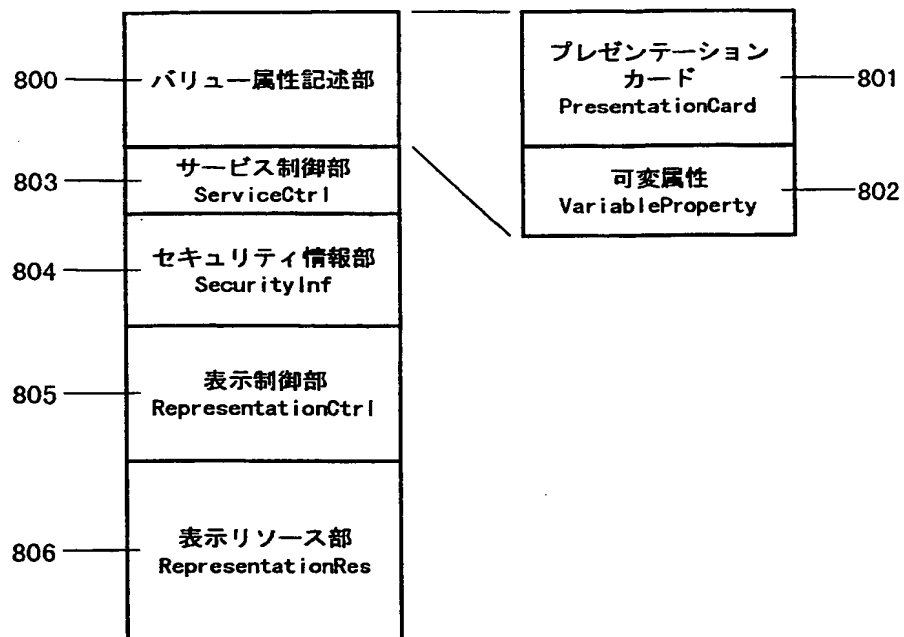
図 1 2



THIS PAGE BLANK (USPTO)

13 / 37

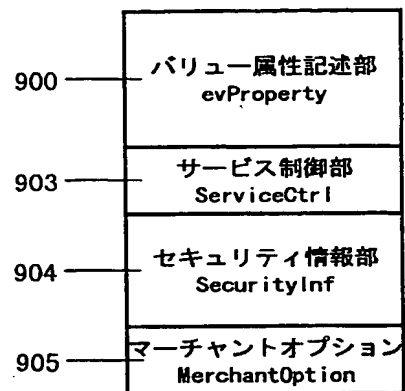
図 13



THIS PAGE BLANK (USPTO)

14 / 37

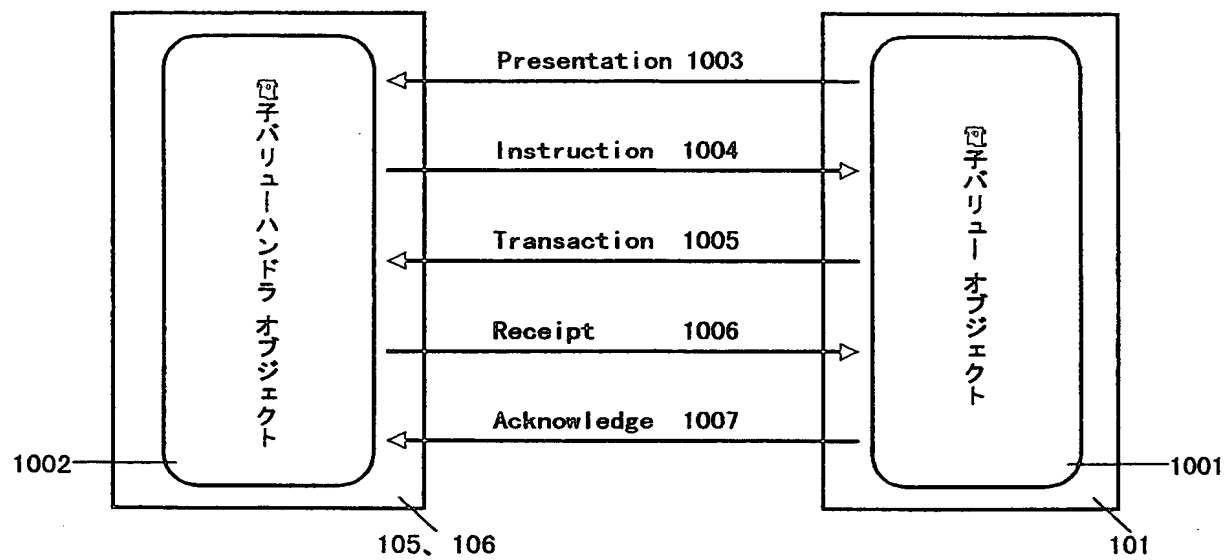
図 14



THIS PAGE BLANK (USPTO)

1 5 / 3 7

図 1 5



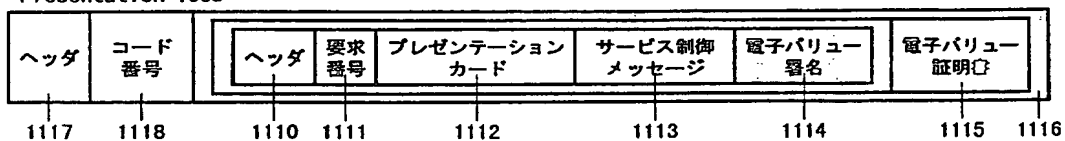
THIS PAGE BLANK (USPTO)

16 / 37

図 16

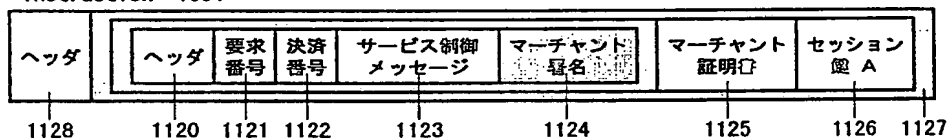
(a)

Presentation 1003



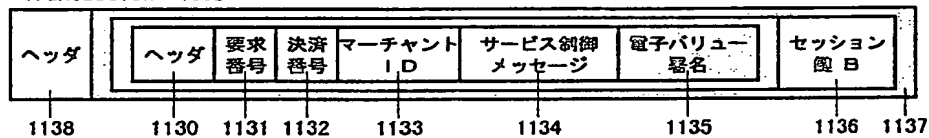
(b)

Instruction 1004



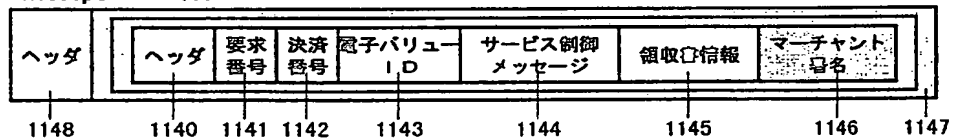
(c)

Transaction 1005



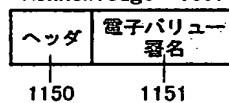
(d)

Receipt 1006



(e)

Acknowledge 1007



THIS PAGE BLANK (USPTO)

图 17

```

<EVMIL version="0.1">
<Description about="wallet:///EValue/ev00000033">
<SignedDescription about="PresentationCard" evID="10000000000000000000000000000001">
: (省略)
<Signer rdf:resource="http://www.evalue.com"/>
<Signature>0123456789</Signature>
</SignedDescription>
— プレゼンテーションカード 801

<SignedDescription about="VariableProperty" evID="10000000000000000000000000000001">
: (省略)
<Signer rdf:resource="http://www.evalue.com/evalue/10000000000000000000000000000001">
<Signature>123456789A</Signature>
</SignedDescription>
— 可変属性 802

<SignedDescription>
<Description about="ServiceCtrl" evID="10000000000000000000000000000001">
: (省略)
</Description>
— サービス制御部 803

<Description about="SecurityInf" evID="10000000000000000000000000000001">
: (省略)
</Description>
— セキュリティ情報部 804

<Description about="RepresentationCtrl" evID="10000000000000000000000000000001">
rdf:resource="http://www.evalue.com/evalue/ev_00003000000000201/RpCtrl"/>
— 表示制御部 805

<Description about="RepresentationRes" evID="10000000000000000000000000000001">
rdf:resource="http://www.evalue.com/evalue/ev_00003000000000201/RpRes"/>
— 表示リソース部 806

<SignedTime>1999.09.07T12:15:07+0900</SignedTime>
<Signer rdf:resource="http://www.evalue.com"/>
<Signature>23456789AB</Signature>
</SignedDescription>

<SignedDescription about="http://www.evalue.com/evalue/ev_00003000000000201/RpCtrl"
evID="10000000000000000000000000000001">
: (省略)
<Signer rdf:resource="http://www.evalue.com"/>
<Signature>3456789ABC</Signature>
</SignedDescription>
— 表示制御部 (実体) 1201

<Description about="http://www.evalue.com/evalue/ev_00003000000000201/RpRes"
evID="10000000000000000000000000000001">
: (省略)
</Description>
— 表示リソース部 (実体) 1202

<Description about="http://www.evalue.com">
<EntityName>Mobile Ticket Service</EntityName>
<EntityID>00000000000000000000000000000001</EntityID>
<Email>ev_issuer@evalue.com</Email>
<Telnum>81-3-5460-x000</Telnum>
</Description>
— サービス提供者
に関する記述 1200
</EVMIL>

```

THIS PAGE BLANK (USPTO)

18 / 37

☒ 18

```
<SignedDescription about="PresentationCard" evID="10000000000000000000000000000001">
  <evType>ticket</evType>
  <evCode>0000300000000201</evCode>
  <evID>10000000000000000000000000000001</evID>
  <evName>Soccer 200X Ticket</evName>
  <evConditionBitmap>0000000000000001</evConditionBitmap>
  <evProp name="TITLE" value="Soccer 200X Japan vs Brazil"/>
  <evProp name="DATE" value="2002.06.30T14:00+0900"/>
  <evProp name="GATE_OPEN" value="2002.06.30T10:00+0900"/>
  <evProp name="LOCATION_NAME" value="Yokohama"/>
  <evProp name="LOCATION_URI" value="http://www.yis.co.jp/map"/>
  <evProp name="SEAT_NUM" value="SS-A-28"/>
  <evProp name="SEAT_POS" value="http://www.mts.com/ticket123/seat/SS-A-28"/>
  <evProp name="SPONSOR_NAME" value="WORLD FOOTBALL ASSOCIATION"/>
  <evProp name="SPONSOR_URI" value="http://www.wfa.org"/>
  <evProp name="CONTACT_TELNUM" value="+81-3-5460-xxxx"/>
  <evProp name="CONTACT_URI" value="http://www.mts.com/contact"/>
  <evProp name="ISSUER_NAME" value="Mobile Ticket Service"/>
  <evProp name="ISSUER_URI" value="http://www.mts.com"/>
  <evProp name="MESSAGE_1" value="No Dangerous Objects"/>
  <SignedTime>1999.09.07T12:15:07+0900</SignedTime>
  <Signer rdf:resource="http://www.evalue.com"/>
  <Signature>0123456789</Signature>
</SignedDescription>
```

```
<SignedDescription about="VriableProperty" evID="10000000000000000000000000000001">
  <evFlag VALIDITY=1 USED=0/>
  <evProp name="USE_SERIAL" value=0/>
  <evProp name="NUMBER" value=1/>
  <evProp name="START_VALID" value="1999.07.23T00:00+0900"/>
  <evProp name="END_VALID" value="2002.06.30T23:59+0900"/>
  <evProp name="MESSAGE_2" value=/>
  <SignedTime>1999.09.07T12:15:07+0900</SignedTime>
  <Signer rdf:resource="http://www.evalue.com/evalue/10000000000000000000000000000001"/>
  <Signature>123456789A</Signature>
</SignedDescription>
```

THIS PAGE BLANK (USPTO)

19 / 37

图 19

```
<Description about="ServiceCtrl" evID="10000000000000000000000000000001">
  <SC-module type="ticket" ID=1 number=$NUMBER start=$START_VALID end=$END_VALID
    used_flag=$USED validity_flag=$VALIDITY serial=$USE_SERIAL/>
  <SC-module type="verify_prop" ID=2 prop=$SEAT_NUM/>
  <SC-module type="set_message" ID=3 msg=$MESSAGE_2/>
</Description>

<Description about="SecurityInf" evID="10000000000000000000000000000001">
  <evOwner>
    <Description about="http://www.evalue.com/user/11000000000000000000000000000001"
      EntityName="Taro Suzuki"
      EntityID="11000000000000000000000000000001"/>
  </evOwner>
  <evResource>http://www.evalue.com/evalue/10000000000000000000000000000001</evResource>
  <evCertificate>
    0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF
  </evCertificate>
  <evPrivateKey>0123456789</evPrivateKey>
  <evAuthKey>0123456789ABCDEF</evAuthKey>
  <evhandlerAuthKey>ABCDEF0123456789</evhandlerAuthKey>
</Description>
```

THIS PAGE BLANK (USPTO)

20 / 37

20

```

<SignedDescription about="http://www.evaluate.com/evaluate/ev_0000300000000201/RpCtrl"
  evID="10000000000000000000000000000001">
  <OptimumRpCtrl>
    <Description about="http://www.evaluate.com/evaluate/ev_0000300000000201/RpCtrl_M01">
      <RpType>MOBILE 01</RpType>
      <RepresentaionCtrlData>
        <CARD name="Main">
          <HAEAD>
            <TITLE><evP>$TITLE</evP></TITLE>
          </HAEAD>
          <BODY>
            <Do type="ACCEPT">
              <Go HREF="wallet:///evTransact"/>
            </Do>
            <CENTER><H1><evP>$TITLE</evP></H1></CENTER>
            <BR><CENTER><IMG SRC="wallet:///evResource label=MAIN_IMG"></CENTER>
            <BR><UL>Date: <evP>$DATE</evP>
            <BR>Stadium: <A HREF=<evP>$LOCATION_URI</evP>><evP>$LOCATION_NAME</evP></A>
            <BR>Seat: <A HREF=<evP>$SEAT_POS</evP>><evP>$SEAT_NUM</evP></A>
            <BR><A HREF="Detail">Details</A></UL>
          </BODY>
        </CARD>
        <CARD name="Detail">
          <HAEAD>
            <TITLE><evP>$TITLE</evP></TITLE>
          </HAEAD>
          <BODY>
            <Do type="ACCEPT">
              <Go HREF="wallet:///evTransact"/>
            </Do>
            <CENTER><H1><evP>$TITLE</evP></H1></CENTER>
            <BR><UL>Date: <evP>$DATE</evP>
            <BR>Open Gate: <evP>$GATE_OPEN</evP>
            <BR>Stadium: <A HREF=<evP>$LOCATION_URI</evP>><evP>$LOCATION_NAME</evP></A>
            <BR><A HREF="wallet:///evResource label=MAP">Map</A>
            <BR>Seat: <A HREF=<evP>$SEAT_POS</evP>><evP>$SEAT_NUM</evP></A>
            <BR>Term of Validity: <evV>$START_VALID</evV> - <evV>$END_VALID</evV>
            <BR>Sponsor: <A HREF=<evP>$SPONSOR_URI</evP>><evP>$SPONSOR_NAME</evP></A>
            <BR>Contact: <A HREF="telephone:///dial num=<evP>$CONTACT_TELNUM</evP>">
              <evP>$CONTACT_TELNUM</evP></A>
            <BR>Issuer: <A HREF=<evP>$ISSUER_URI</evP>><evP>$ISSUER_NAME</evP></A>
            <BR><evP>$MESSAGE_1</evP>
            <BR><evV>$MESSAGE_2</evV>
            <BR><A HREF="Main">Top Page</A></UL>
          </BODY>
        </CARD>
      </RepresentaionCtrlData>
    </Description>
  </OptimumRpCtrl>
  <SignedTime>1999.09.07T12:15:07+0900</SignedTime>
  <Signer rdf:resource="http://www.evaluate.com"/>
  <Signature>3456789ABC</Signature>
</SignedDescription>

```

THIS PAGE BLANK (USPTO)

图 2 1

```
<Description about="http://www.evalue.com/evalue/ev_00003000000000201/RpRes"  
    evID="100000000000000000000000000000001">  
    <OptimumRpRes>  
        <Image>  
            URI="http://www.evalue.com/resources/0123456789ABCDEF"  
            label="MAIN_IMG"  
            type="jpeg"  
            data="1202A846574A63D946 ..... (省略) ..... B48364605987F687543"  
        </Image>  
        <Image>  
            URI="http://www.evalue.com/resources/123456789ABCDEF0"  
            label="MAP"  
            type="jpeg"  
            data="202A846574A63D946B ..... (省略) ..... 48364605987F687543F"  
        </Image>  
        <Sound>  
            URI="http://www.evalue.com/resources/23456789ABCDEF01"  
            label="Greet"  
            type="mp3"  
            data="1202A846574A63D946 ..... (省略) ..... B48364605987F687543"  
        </Sound>  
    </OptimumRpRes>  
</Description>
```

THIS PAGE BLANK (USPTO)

2 2 / 3 7

☒ 2 2

```
<EVML version="0.1">
  <CARD name="Main">
    <HAEAD>
      <TITLE>Soccer 200X Japan vs Brazil </TITLE>
    </HAEAD>
    <BODY>
      <Do type="ACCEPT">
        <Go HREF="wallet:///evTransact"/>
      </Do>
      <CENTER><H1>Soccer 200X Japan vs Brazil </H1></CENTER>
      <BR><CENTER><IMG SRC="wallet:///evResource label=MAIN_IMG"></CENTER>
      <BR><UL>Date: 2002.06.30T14:00+0900
      <BR>Stadium: <A HREF="http://www.yis.co.jp/map"> Yokohama </A>
      <BR>Seat: <A HREF="http://www.mts.com/ticket123/seat/SS-A-28"> SS-A-28</A>
      <BR><A HREF="Detail">Details</A></UL>
    </BODY>
  </CARD>
</EVML>
```

THIS PAGE BLANK (USPTO)

2 3 / 3 7

☒ 2 3

<EVMML version="0.1">

<Description about="evMerchant//evHandler/evh00000001">

<SignedDescription>

<Description about="evProperty" evhandlerID="20000000000000000000000000000001">

<evType>ticket</evType>

<evCode>0000300000000201</evCode>

<evhandlerID>20000000000000000000000000000001</evhandlerID>

<evName>Soccer 200X Ticket</evName>

<evConditionBitmap>0000000000000001</evConditionBitmap>

<evProp name="TITLE" value="Soccer 200X Japan vs Brazil"/>

<evProp name="DATE" value="2002.06.30T14:00+0900"/>

<evProp name="GATE_OPEN" value="2002.06.30T10:00+0900"/>

<evProp name="LOCATION_NAME" value="Yokohama"/>

<evProp name="LOCATION_URI" value="http://www.yis.co.jp/map"/>

<evProp name="SEAT_NUM" value="permission="public"/>

: (省略)

<evProp name="MESSAGE_2" value="permission="public"/>

</Description>

バリュー属性記述部 900

<Description about="ServiceCtrl" evhandlerID="20000000000000000000000000000001">

<SC-module type="ticket" ID=1 number=\$NUMBER start=\$START_VALID end=\$END_VALID
used_flag=\$USED validity_flag=\$VALIDITY serial=\$USE_SERIAL />

<SC-module type="verify_prop" ID=2 prop=\$SEAT_NUM/>

<SC-module type="set_message" ID=3 msg=\$MESSAGE_2/>

</Description>

サービス制御部 903

<Description about="SecurityIn" evhandlerID="20000000000000000000000000000001">

<evhandlerOwner>

<Description about="http://www.evalue.com/merchant/21000000000000000000000000000001">

EntityName="ABC Event Service"

EntityID="21000000000000000000000000000001"/>

</evhandlerOwner>

<evResource>http://www.evalue.com/evhandler/20000000000000000000000000000001

</evResource>

<evAuthKey>0123456789ABCDEF</evAuthKey>

<evhandlerAuthKey>ABCDEF0123456789</evhandlerAuthKey>

</Description>

セキュリティ情報部 904

<SignedTime>1999.09.07T12:15:07+0900</SignedTime>

<Signer>

<Description about="http://www.evalue.com">

<EntityName>Mobile Ticket Service</EntityName>

<EntityID>00000000000000000000000000000001</EntityID>

<Email>ev_issuer@evalue.com</Email>

<Telnum>81-3-5460-xxxx</Telnum>

</Description>

</Signer>

<Signature>23456789AB</Signature>

</SignedDescription>

<Description about="MerchantOption" evhandlerID="20000000000000000000000000000001">

<SetevProp>\$SEAT_NUM="SS-"/>

<SetevProp>\$MESSAGE_2="Special News available: http://www.yis.co.jp/news/20020630"

</SetevProp>

</Description>

マーチャントオプション

</Description>

905

</EVMML>

THIS PAGE BLANK (USPTO)

2 4 / 3 7

☒ 2 4

(a)

```
<SC-MSG>
  <scm_msg ID=1 number=1 start="1999.07.23T00:00+0900" end="2002.06.30T23:59+0900"
    used_flag=0 validity_flag=1 serial=0/>
  <scm_msg ID=2 prop="SS-A-28"/>
  <scm_msg ID=3 msg=/>
</SC-MSG>
```

(b)

```
<SC-MSG>
  <scm_msg ID=1 number=0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+0900"
    used_flag=1 validity_flag=1 serial=1/>
  <scm_msg ID=3 msg="Special News available: http://www.yis.co.jp/news/20020630/"/>
</SC-MSG>
```

(c)

```
<SC-MSG>
  <scm_msg ID=1 number=0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+0900"
    used_flag=1 validity_flag=1 serial=1/>
  <scm_msg ID=2 prop="SS-A-28"/>
  <scm_msg ID=3 msg="Special News available: http://www.yis.co.jp/news/20020630/"/>
</SC-MSG>
```

(d)

```
<SC-MSG>
  <scm_msg ID=1 serial=1/>
</SC-MSG>
```

THIS PAGE BLANK (USPTO)

2 5 / 3 7

図 2 5

```
<SignedDescription about="VariableProperty" evID="10000000000000000000000000000001">
  <evFlag VALIDITY=1 USED=1/>
  <evProp name="USE_SERIAL" value=1/>
  <evProp name="NUMBER" value=0/>
  <evProp name="START_VALID" value="2002.06.30T12:25+0900"/>
  <evProp name="END_VALID" value="2002.06.30T23:59+0900"/>
  <evProp name="MESSAGE_2" value="Special News available: http://www.yis.co.jp/news/20020630/">
  <SignedTime>2002.06.30T12:25+0900</SignedTime>
  <Signer rdf:resource="http://www.evalue.com/evalue/10000000000000000000000000000001"/>
  <Signature>A12345678A</Signature>
</SignedDescription>
```

THIS PAGE BLANK (USPTO)

26 / 37

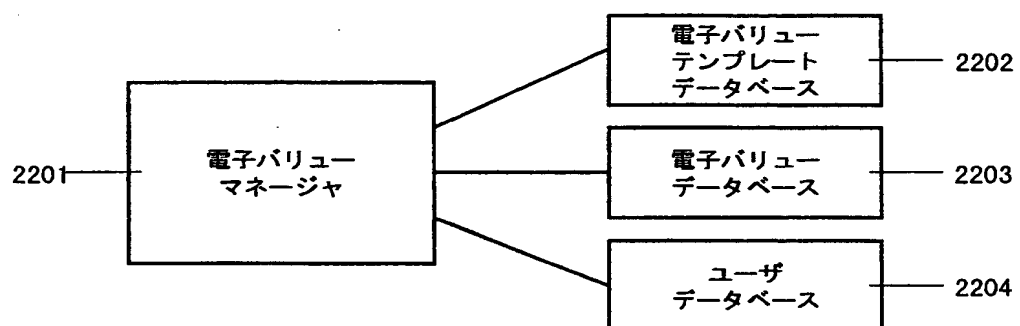
図 26

```
<EVMML version="0.1">
  <CARD name="Receive EV">
    <HAEAD>
      <TITLE>Receive Electronic Value</TITLE>
    </HAEAD>
    <BODY>
      Your order was accepted.
    <BR>
    <CENTER>
      <H1>
        <Go HREF="wallet:///evReceive">
          <param name="EV_ISSUER_URI" value="http://www.evalue.com"/>
          <param name="SESSION_NUM" value="a01b23c45d67e89f"/>
          Receive e-Value
        </Go>
      </H1>
    </CENTER>
    </BODY>
  </CARD>
</EVMML>
```

THIS PAGE BLANK (USPTO)

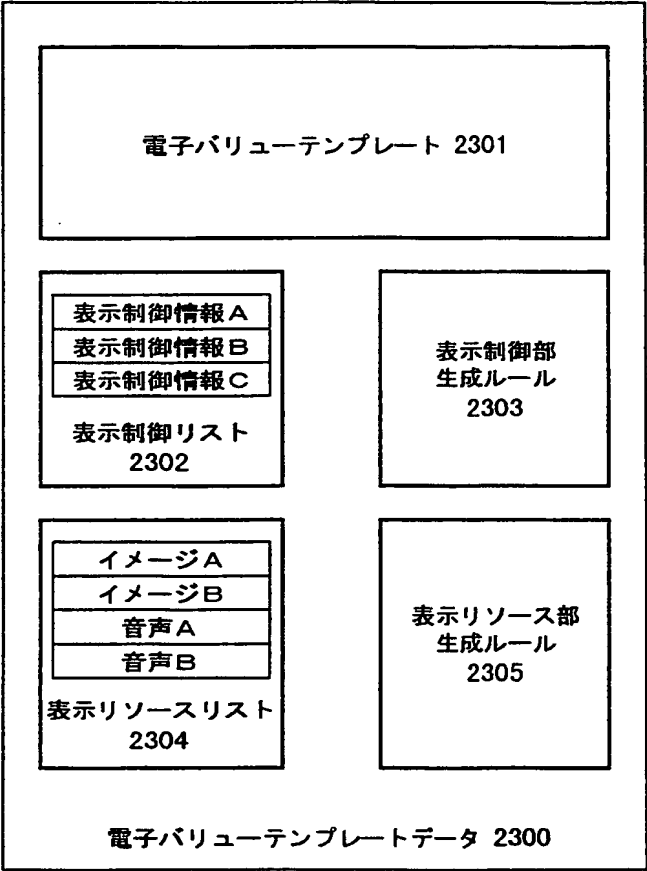
27 / 37

図 27



THIS PAGE BLANK (USPTO)

図 28

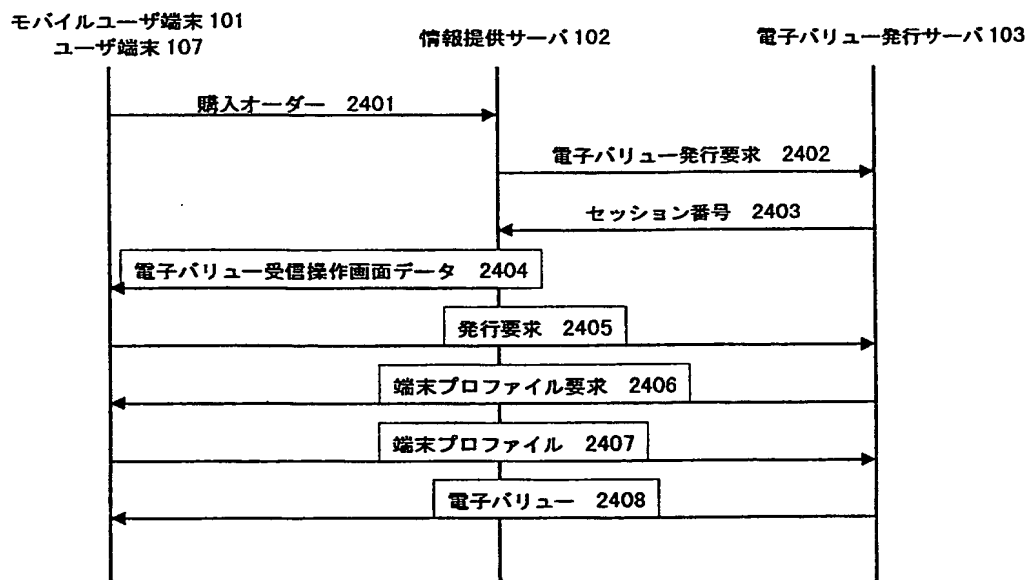


THIS PAGE BLANK (USPTO)

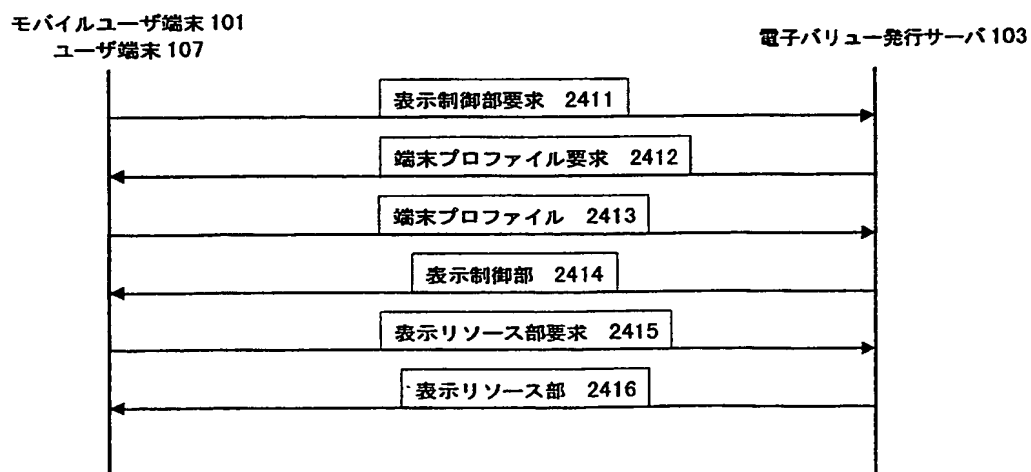
29 / 37

図 29

(a)



(b)



THIS PAGE BLANK (USPTO)

30 / 37

図 30

(a)

```
<Description about="evissuingRequest" ID="100000000000123">
  <evType>ticket</evType>
  <evCode>0000300000000201</evCode>
  <evProp name="SEAT_NUM" value="SS-A-28"/>
  <evProp name="SEAT_POS" value="http://www.mts.com/ticket123/seat/SS-A-28"/>
</Description>
```

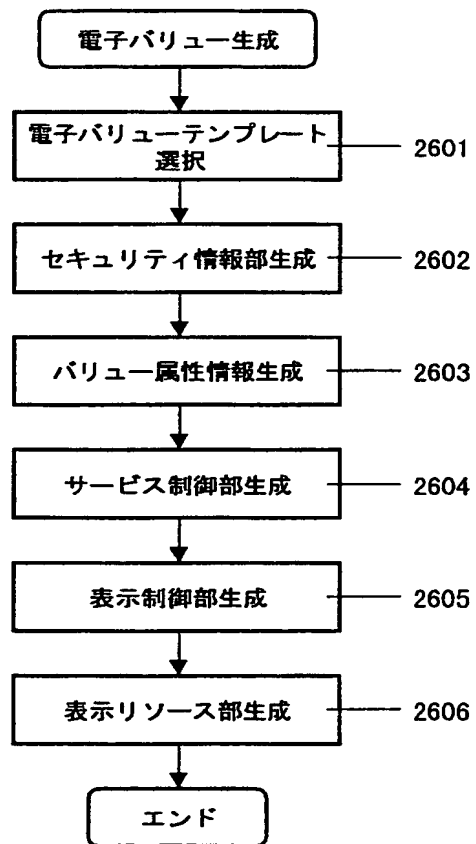
(b)

```
<Description about="TerminalProfile">
  <TerminalType>MT0001</TerminalType>
  <BrowserType>B000B20A</BrowserType>
  <eWalletType>W000A10B</eWalletType>
  <Screen>160x200x8</Screen>
</Description>
```

THIS PAGE BLANK (USPTO)

31 / 37

図 31



THIS PAGE BLANK (USPTO)

图 3 2

```

<EVMML version="0.1">
  <Description about="http://www.evalue.com/evalue/10000000000000000000000000000001">
    <SignedDescription about="PresentationCard" evID="10000000000000000000000000000001">
      : (省略)
      <Signer rdf:resource="http://www.evalue.com"/>
      <Signature>0123456789</Signature>
    </SignedDescription>
  </Description>
  <Description about="VariableProperty" evID="10000000000000000000000000000001">
    : (省略)
    <Signer rdf:resource="http://www.evalue.com/evalue/10000000000000000000000000000001">
    <Signature>123456789A</Signature>
  </SignedDescription>
  <SignedDescription>
    <Description about="ServiceCtrl" evID="10000000000000000000000000000001">
      : (省略)
    </Description>
    <Description about="SecurityInf" evID="10000000000000000000000000000001">
      : (省略)
    </Description>
    <Description about="RepresentaionCtrl" evID="10000000000000000000000000000001"
      rdf:resource="http://www.evalue.com/evalue/ev_00003000000000201/RpCtrl"/>
    </Description>
    <Description about="RepresentaionRes" evID="10000000000000000000000000000001"
      rdf:resource="http://www.evalue.com/evalue/ev_00003000000000201/RpRes"/>
    </Description>
    <SignedTime>1999.09.07T12:15:07+0900</SignedTime>
    <Signer rdf:resource="http://www.evalue.com"/>
    <Signature>23456789AB</Signature>
  </SignedDescription>
  <SignedDescription about="http://www.evalue.com/evalue/ev_00003000000000201/RpCtrl"
    evID="10000000000000000000000000000001">
    : (省略)
    <Signer rdf:resource="http://www.evalue.com"/>
    <Signature>3456789ABC</Signature>
  </SignedDescription>
  <Description about="http://www.evalue.com/evalue/ev_00003000000000201/RpRes"
    evID="10000000000000000000000000000001">
    : (省略)
  </Description>
  <Description about="http://www.evalue.com">
    <EntityName>Mobile Ticket Service</EntityName>
    <EntityID>00000000000000000000000000000001</EntityID>
    <Email>ev_issuer@evalue.com</Email>
    <Telnum>81-3-5460-xxxx</Telnum>
  </Description>
</EVMML>

```

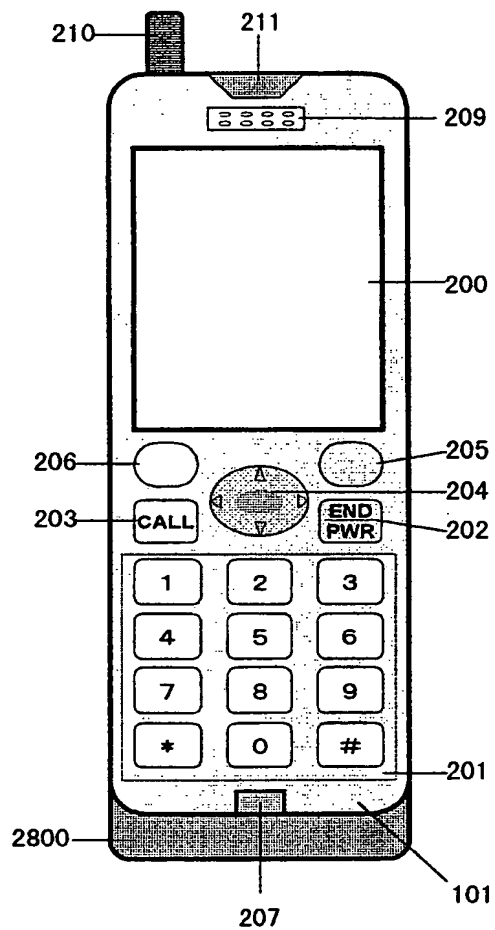
プレゼンテーション
カード 801
 可変属性 802
 サービス制御部 803
 セキュリティ情報部 804
 表示制御部 805
 表示リソース部 806
 表示制御部 (実体) 1201
 表示リソース部 (実体) 1202
 サービス提供者
に関する記述 1200

THIS PAGE BLANK (USPTO)

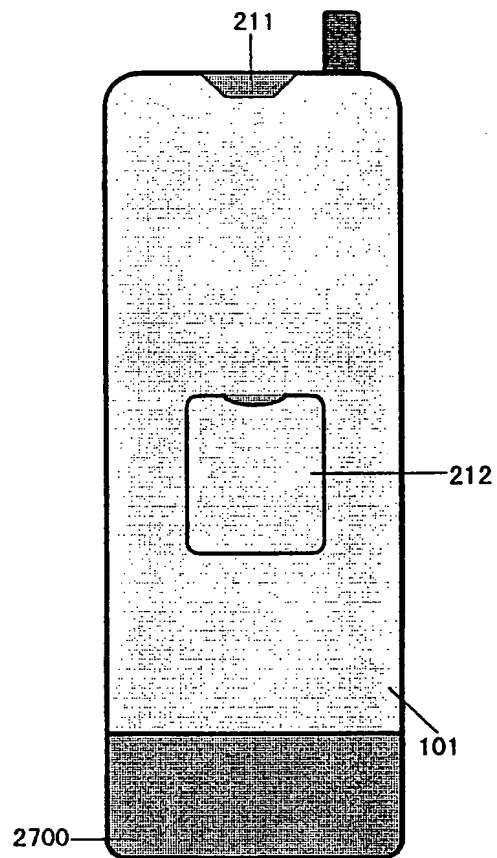
33 / 37

図 33

(a)



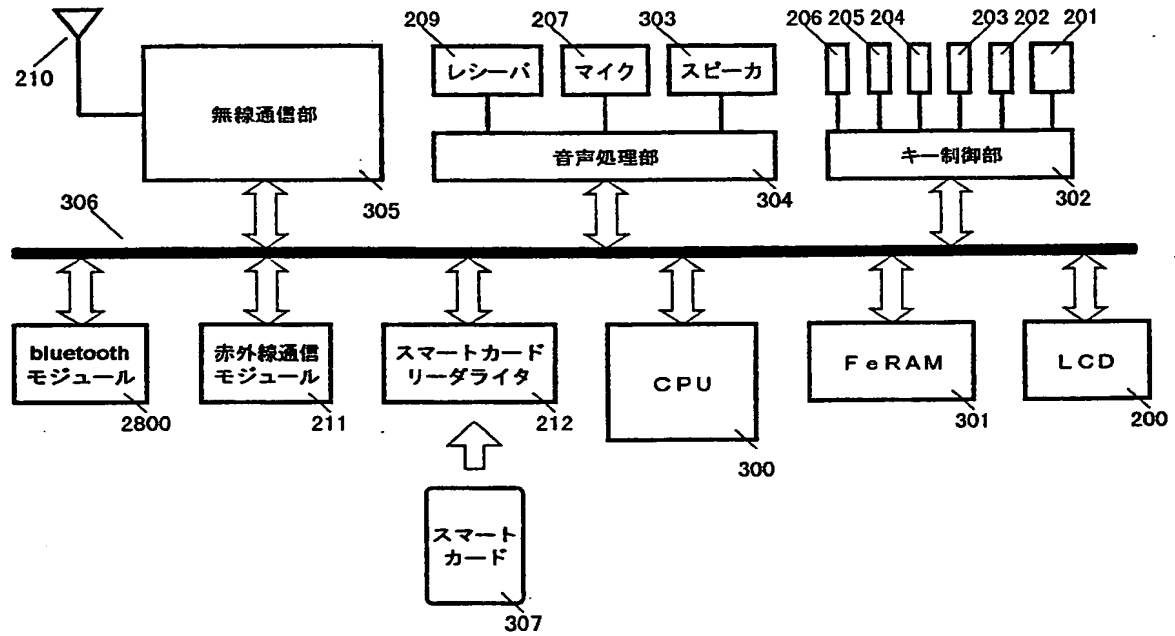
(b)



THIS PAGE BLANK (USPTO)

34 / 37

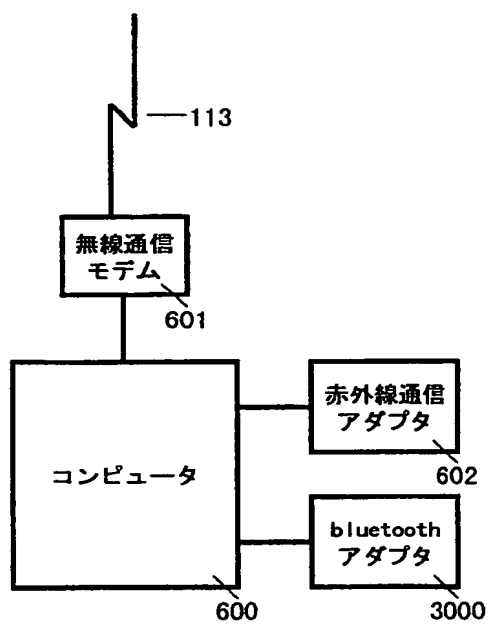
図 34



THIS PAGE BLANK (USPTO)

35 / 37

図 35



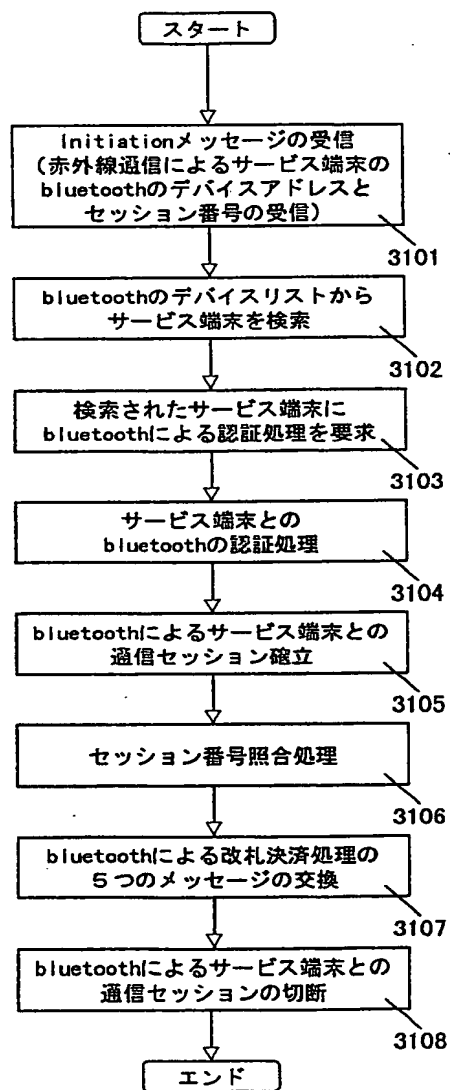
THIS PAGE BLANK (USPTO)



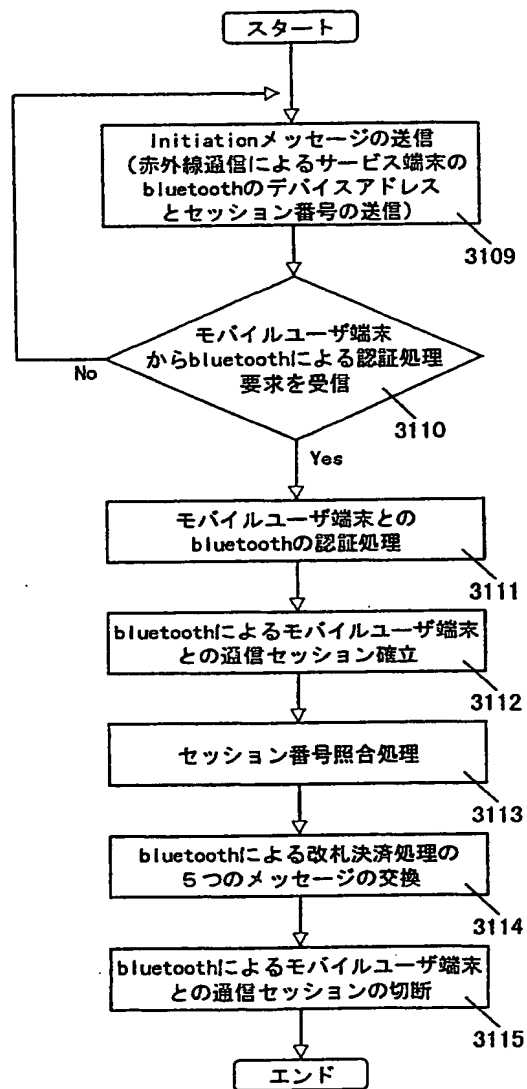
36 / 37

図 36

(a) モバイルユーザ端末



(b) サービス端末



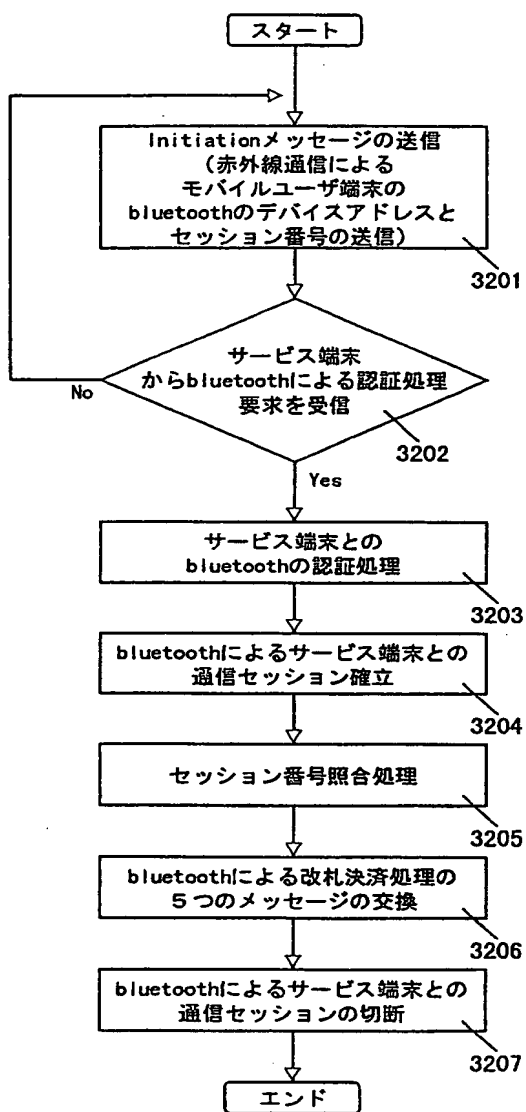
THIS PAGE BLANK (USPTO)



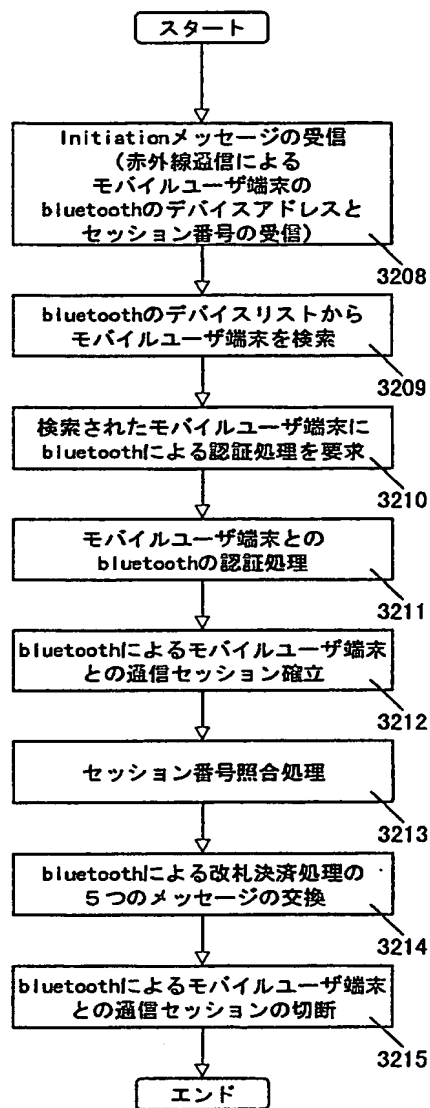
37 / 37

図 37

(a) モバイルユーザ端末



(b) サービス端末



THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06355

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F 17/60 G06F 19/00 G07F 7/08 G09C 1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
 Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WAYNER, Peter, Digital Cash: Commerce on the Net, 2 nd edition, 01 April, 1997 (01.04.97), Academic Press (London, UK). See the "Migration" section on pp. 212-213 (especially, the paragraphs "For instance, the first batch of...", "Mondex clearly anticipates updating...").	1
X	WO, 99/09502, A1 (Mataushita Electric Industrial Co., Ltd.), 25 February, 1999 (25.02.99), & AU, 86484/98, A1 & CN, 1246941, A & EP, 950968, A1 & JP, 99/09502, A1 See Figs. 109(b), 110(a) (b) (especially [10915], [11006]; cf. Fig. 19 [1098])	18-20, 25, 26
X	JP, 11-225143, A (Fuji Xerox Co., Ltd.), 17 August, 1999 (17.08.99), (Family: none) See the description of working examples 2, 3 (especially, of M, M', x)	25
A	JP, 11-032104, A (Fuji Xerox Co., Ltd.), 02 February, 1999 (02.02.99), (Family: none)	1-35

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
12 December, 2000 (12.12.00)Date of mailing of the international search report
26 December, 2000 (26.12.00)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06355

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	<i>See the description of "the 3rd protocol" (especially, i, i_n).</i>	
A	GLASSMAN, Steve et al., "The Millicent Protocol for Inexpensive Electronic Commerce", in <i>World Wide Web Journal-Fourth international World Wide Web Conference</i> , December 1995, O'Reilly & Associates (Sebastopol, USA). <i>See Appendix (especially, "Authentic and private.")</i>	1-35
A	EP, 917120, A2, A3 (Citicorp Development Center Inc.), 19 May, 1999 (19.05.99), & AU, 92346/98, A1 & AU, 17965/99, A1 & AU, 15844/99, A1 & BR, 98/06416, A & CN, 1233804, A & EP, 951158, A2 & EP, 950992, A2, A3 & EP, 917119, A2 & JP, 11-232348, A & JP, 11-250165, A & WO, 99/24891, A2 & WO, 99/24891, A2 <i>See Fig. 3 (especially, 2 "applications container.")</i>	1-35
A	FINGER, Peter et al., "The Business of Distributed Object Computing," in <i>Object Magazine</i> , April 1997 (04.97). <i>See the paragraph "The bottom layers provides..."</i>	1-35

国際調査報告

国際出願番号 PCT/JPO0/06355

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. CL⁷ G06F 17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. CL⁷ G06F 17/60 G06F 19/00 G07F 7/08 G09C 1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926 - 1996 年
 日本国公開実用新案公報 1971 - 2000 年
 日本国実用新案登録公報 1996 - 2000 年
 日本国登録実用新案公報 1994 - 2000 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WAYNER, Peter, <i>Digital Cash: Commerce on the Net</i> , 2nd edition, April 1 1997 (01.04.97), Academic Press (London, UK). pp. 212-213 の "Migration" セクションを見よ (特に "For instance, the first batch of ..." と "Mondex clearly anticipates updating..." の段落).	1
X	WO, 99/09502, A1 (松下電器産業株式会社) 25.2 月.1999 (25.02.99) & AU, 86484/98, A1 & CN, 1246941, A	18-20, 25, 26

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

12.12.00

国際調査報告の発送日

26.12.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

阿波 進

5 L

9168

電話番号 03-3581-1101 内線 3561

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	& EP, 950968, A1 & JP, 99/09502, A1 図 109(b)と 110(a)(b)を見よ(特に[10915]と[11006]; cf. 図 19 [1098]).	
X	JP, 11-225143, A (富士ゼロックス株式会社) 17.8 月.1999 (17.08.99) (ファミリーなし) 実施例 2 および 3 の記述を見よ(特に M, M', および x の扱いについて).	25
A	JP, 11-031204, A (富士ゼロックス株式会社) 2.2 月.1999 (02.02.99) (ファミリーなし) 「第 3 のプロトコル」の記述を見よ(特に i と in の扱いについて).	1-35
A	GLASSMAN, Steve <i>et al</i> , "The Millicent Protocol for Inexpensive Electronic Commerce", in <i>World Wide Web Journal—Fourth International World Wide Web Conference</i> , December 1995, O'Reilly & Associates (Sebastopol, USA). <i>Appendix</i> を見よ(特に "Authentic and private" の項目).	1-35
A	EP, 917120, A2, A3 (Citicorp Development Center Inc) 19. 5 月. 1999 (19.05.99) & AU, 92346/98, A1 & AU, 17965/99, A1 & AU, 15844/99, A1 & BR, 98/06416, A & CN, 1233804, A & EP, 951158, A2 & EP, 950992, A2, A3 & EP, 917119, A2 & JP, 11-232348, A & JP, 11-250165, A & WO, 99/24891, A2 & WO, 99/24891, A2 図 3 を見よ(特に 2 つの "applications container" について).	1-35
A	FINGAR, Peter <i>et al</i> , "The Business of Distributed Object Computing",	1-35

THIS PAGE BLANK (USPTO)

C (続き) . 関連すると認められる文献		関連する 請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
	<p>in <i>Object Magazine</i>, April 1997 (04.97).</p> <p>"<i>The bottom layers provides ...</i>" の段落を見よ.</p>	

THIS PAGE BLANK (USPTO)